

UNIVERSIDADE FEDERAL DE MINAS GERAIS
FACULDADE DE DIREITO

**ENTRE O SABER E O SEGREDO: uma leitura realista da tolerância
da espionagem internacional na era do medo**

Belo Horizonte
2017

UNIVERSIDADE FEDERAL DE MINAS GERAIS
FACULDADE DE DIREITO

**ENTRE O SABER E O SEGREDO: uma leitura realista da tolerância
da espionagem internacional na era do medo**

Tese de doutorado apresentada pelo candidato
Humberto Alves de Vasconcelos Lima ao
Programa de Pós-Graduação em Direito da
Universidade Federal de Minas Gerais como
requisito para obtenção do grau de Doutor em
Direito.

Belo Horizonte

2017

L732e Lima, Humberto Alves de Vasconcelos
Entre o saber e o segredo: uma leitura realista da tolerância
da espionagem internacional na era do medo / Humberto Alves
de Vasconcelos Lima – 2016.

Orientador: Roberto Luiz Silva.
Tese (doutorado) – Universidade Federal de Minas
Gerais, Faculdade de Direito.

1. Direito internacional – Teses 2. Espionagem 3. Serviço de
inteligência 4. Relações internacionais 5. Soberania I. Título

CDU₍₁₉₇₆₎ 341.326

Entre o saber e o segredo: uma leitura realista da tolerância da espionagem internacional na era do medo

Tese de doutorado apresentada pelo candidato **Humberto Alves de Vasconcelos Lima** ao Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais como requisito para obtenção do grau de Doutor em Direito.

Comissão examinadora:

Professor Doutor Roberto Luiz Silva (Orientador)
Universidade Federal de Minas Gerais

Professor Doutor Aziz Tuffi Saliba
Universidade Federal de Minas Gerais

Professor Doutor Fabrício Bertini Pasquot Polido
Universidade Federal de Minas Gerais

Professor Doutor Paulo Roberto de Almeida
Centro Universitário de Brasília

Professor Doutor André de Carvalho Ramos
Universidade de São Paulo

Professor Doutor Marcelo Andrade Féres (Suplente)
Universidade Federal de Minas Gerais

Professor Doutor Fabiano Teodoro de Rezende Lara (Suplente)
Universidade Federal de Minas Gerais

Tese _____ em, _____ de _____ de _____.
Belo Horizonte. Faculdade de Direito da Universidade Federal de Minas Gerais.

AGRADECIMENTOS

Inicialmente agradeço aos meus familiares: meus pais Ovídio e Marilda, meus irmãos Adriano e Vanessa e minha esposa Flávia.

Agradeço ao Professor Roberto Luiz Silva por ter conduzido a orientação com seriedade, lendo todos os textos que produzi com atenção e em profundidade e tecendo comentários que refletiram diretamente na tese. O encorajamento que expressou durante todo o período da orientação foi realmente importante para que eu prosseguisse na trajetória acadêmica.

Agradeço também ao Professor Aziz Tuffi Saliba, quem acompanha meu trabalho desde a graduação, quando foi meu orientador, tal como no mestrado. Durante esse longo período se acumularam muitas razões para lhe agradecer, todas elas relacionadas sempre com manifestações de apoio, hoje sintômas de uma sólida amizade.

Agradeço ao Professor Fabrício Bertini Pasquot Polido, sempre solícito quando convidado a participar das bancas. A leitura atenta e detalhada que fez do trabalho resultou em críticas valiosas e decisivas para a correção de alguns equívocos. Além disso, a organização dos “Seminários de Governança das Redes” ofereceu um excelente espaço para que eu pudesse discutir temas relacionados a espionagem cibernética. Aproveito para agradecer aos Professores Paulo Roberto de Almeida e André de Carvalho Ramos por gentilmente terem aceitado o convite para compor a banca examinadora.

Entre os colegas, agradeço aos que se tornaram amigos: Ana Luísa Peres e Letícia Daibert, pelos momentos de descontração que ajudaram a aliviar a tensão de um curso de doutorado. Agradeço também ao Tarcísio Diniz Magalhães, com quem pude discutir temas de Relações Internacionais que repercutiram na tese e ao Reinaldo Luz, com quem pude conversar sobre temas de metodologia. Ainda na Faculdade de Direito da UFMG, agradeço aos seus servidores, especialmente os da secretaria, que sempre me atenderam com cordialidade e eficiência.

Por fim, registro o suporte da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), que forneceu o auxílio financeiro necessário para que eu pudesse conduzir a pesquisa em regime de dedicação exclusiva.

Muito obrigado a todos!

RESUMO

Neste trabalho se analisa a atividade da espionagem estatal através do Direito Internacional e das Relações Internacionais. Inicialmente é apresentado um breve estudo propedêutico e descritivo sobre a atividade de inteligência, onde são examinadas suas atribuições, sua estrutura e funcionamento, bem como os mecanismos de controle e fiscalização correspondentes. Posteriormente, é discutido o contexto político atual sobre o qual operam alguns dos principais serviços de inteligência do mundo, quando se argumenta que a retórica da segurança diante de ameaças terroristas do extremismo islâmico foi o principal fator que os impulsionou. São exploradas a seguir as capacidades atuais dos serviços de inteligência e identificados os principais problemas associados a uma estratégia abrangente de coleta de informações. Em diante assume-se postura dogmática para oferecer resposta ao problema da licitude da espionagem internacional em tempo de paz. Nessa análise o problema é estratificado para que se possa examinar criticamente a licitude de diferentes modalidades de espionagem segundo o Direito Internacional, sugerindo-se a seguinte e inédita classificação: a) espionagem de informações privadas de particulares; b) espionagem econômica de segredos de empresa e c) espionagem de segredos de Estado. A tal estratificação corresponde uma análise da licitude da atividade de acordo com os regimes normativos de Direito Internacional em que se inserem, respectivamente: a proteção internacional dos direitos humanos, a proteção internacional da propriedade intelectual, e a proteção da soberania nacional. Desse modo, pretende-se verificar se a espionagem internacional viola cada uma dessas formas de tutela quando têm por objeto os diferentes tipos de informação mencionados. As constatações ali alcançadas são sintetizadas na conclusão de que a escassez de normas de Direito Internacional aplicáveis ao problema da espionagem determina um ambiente de tolerância da atividade, mas que se manifesta em diferentes graus de acordo com a modalidade da atividade. Recorre-se ao estudo das Relações Internacionais para investigar as causas da tolerância da espionagem internacional, o que é feito sob as proposições do realismo político. Isso é precedido de uma proposta de revisitação do realismo através da reavaliação das críticas que a ele são dirigidas. São ainda investigados, também sob o prisma realista, o significado político e as consequências que um ambiente de tolerância da espionagem produz nas relações internacionais. Aqui se identificou que a tolerância da atividade serve à conservação do *status quo* de grandes potências mas, paralelamente, atenua o dilema da segurança ao interferir no grau de incerteza entre os Estados. Por fim, sugere-se que os Estados que possuem capacidades modestas de inteligência devem se reunir em redes de compartilhamento de informações como melhor forma para se alterar o *status quo*.

Palavras-Chave: Inteligência. Espionagem. Direito Internacional. Realismo Político.

ABSTRACT

This paper analyzes state sponsored espionage activities through International Law and International Relations. Initially, a brief introductory and descriptive study of the intelligence service is presented, where its duties, structure and functioning are examined, as well as the corresponding control and oversight mechanisms. Subsequently, the current political context in which some of the greatest world's intelligence services operate is discussed. In this opportunity, we argue that the security rhetoric in the face of terrorist threats of Islamic extremism was the main factor that propelled the capacities of those services. Afterwards, the current capabilities of the intelligence services are explored and the main problems associated with a broad strategy of information gathering are identified. Then, we assume a dogmatic position to provide answers to the problem of peacetime espionage international lawfulness. In this analysis the problem is stratified so that we can critically examine the lawfulness of different types of espionage under International Law, suggesting the following and novel classification: a) espionage of private information from individuals; b) economic espionage of trade secrets; and c) espionage of State secrets. To this classification corresponds an analysis of the lawfulness of the activity under the International Law regimes in which they are inserted, respectively, the international protection of human rights, intellectual property law, and the protection of national sovereignty. Thus, we intended to verify if the international espionage violates each of these forms of protection when it aims the different types of information mentioned. The findings achieved are summarized in the conclusion that the scarcity of rules of International Law applicable to the espionage problem defines a context of tolerance, which is manifested in different degrees, according to the type of the activity. We resort to the study of International Relations to investigate the causes of tolerance of international espionage, what is performed under the propositions of political realism. This is preceded by a proposal of revisiting the realism in light of a revaluation of its opposed criticism. We investigate, also under the realistic perspective, the political significance and the consequences that a context of tolerance of espionage produces in international relations. Here we found that the tolerance supports the preservation of the *status quo* of great powers, but, at the same time, mitigates the security dilemma by interfering with the level of uncertainty among States. Finally, we suggest that States with modest intelligence capacities should ally in information sharing networks as the better strategy for overcome the *status quo*.

Keywords: Intelligence. Espionage. International Law. Political Realism.

LISTA DE SÍGLAS, ACRÔNIMOS, CONTRAÇÕES E CÓDIGOS

ABIN – Agência Brasileira de Inteligência

ABM – Anti-Ballistic Missile

ABNT – Associação Brasileira de Normas Técnicas

AIEA – Agência Internacional de Energia Atômica

BND – Bundesnachrichtendienst

BfV – Bundesamt für Verfassungsschutz

CEDH – Corte Europeia de Direitos Humanos

CIA – Central Intelligence Agency

CIJ – Corte Internacional de Justiça

CNCA – Centro Nacional de Coordinación Antiterrorista

CNE – Computer Network Exploitation

COMINT – Communications Intelligence

CSE – Communications Security Establishment

CPJI – Corte Permanente de Justiça Internacional

CSIS – Canadian Security Intelligence Service

DNI – Digital Network Intelligence

DNR – Dialed Number Recognition

DOE – Department of Energy

DOS - Department of State

DOT - Department of Treasure

DST – Direction de la Surveillance du Territoire

ELINT – Electronic Intelligence

ETA – Euskadi Ta Askatasuna

F/A – Fighter/Attack Aircraft

FBI – Federal Bureau of Investigation

FED – Federal Reserve System

FISA – Foreign Intelligence Surveillance Act

FISC – Foreign Intelligence Surveillance Court

FMI – Fundo Monetário Internacional

FOIA – Freedom of Information Act

FORNSAT – Foreign satellite

FSB – Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii

FVEY – Five Eyes

G-2 – U.S. Army Intelligence

GAO – Global Operation Access

GATT – General Agreement on Tariffs and Trade

GCHQ – Government Communications Headquarters

GRU – Glavnoye Razvedyvatel'noye Upravleniye

HUMINT – Human-Source Intelligence

IMEI – International Mobile Station Equipment Identity

IMINT – Imagery Intelligence

INF – Intermediate-Range Nuclear Forces

IP – Internet Protocol

IRA – Irish Republican Army

ISIS – Islamic State of Iraq and Syria

ITU – International Telecommunication Union

JSOC – Joint Special Operations Command

KGB – Komitet gosudarstvennoy bezopasnosti

KIQs – Key Intelligence Questions

MI5(6) – Military Intelligence 5(6)

NATO – North Atlantic Treaty Organization

NGA – National Geospatial-Intelligence Agency

NIC – National Intelligence Council

NIE – National Intelligence Estimate

NIFC – NATO Intelligence Fusion Centre

NIPF – National Intelligence Priorities Framework

NOCs – Non-Official-Cover Operatives

NRO – National Reconnaissance Office

NSA - National Security Agency

OCDE – Organização para Cooperação Econômica e Desenvolvimento

ODNI – Office of the Director of National Intelligence

OMC – Organização Mundial do Comércio

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte

OSINT – Open-Source Intelligence

PDB – President's Daily Briefing

SALT – Strategic Arms Limitation Treaty

Shin Bet – Sherut ha'Bitachon ha'Klali

SIGINT – Signals Intelligence

SISBIN – Sistema Brasileiro de Inteligência

SNI – Serviço Nacional de Inteligência

SVR – Sluzhba Vnezhney Rasvedki

TAO – Tailored Access Operations

TOR – The Onion Router

TRIPS – Trade-Related Aspects of Intellectual Property Rights

USA PATRIOT ACT – Uniting and Strengthening America by Providing Appropriate
Tools Required to Intercept and Obstruct Terrorism

USAF-ISR – United States Air Force Intelligence, Surveillance, and Reconnaissance
Enterprise

USB – Universal Serial Bus

LISTA DE ANEXOS

Anexo 1 – Iraq’s Continuing Programs for Weapons of Mass Destruction, National Intelligence Estimative, October 2002.

Anexo 2 – “Bin Ladin Determined to Strike US”, President’s Daily Brief, 6 august 2001.

Anexo 3 – U.S. Intelligence Funding

Anexo 4 – In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. D/B/A Verizon Business Services, 19 july 2013.

Anexo 5 – New Collection Posture

Anexo 6 – “Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets”, june 2010.

Anexo 7 – SIGINT Authority decision Tree

Anexo 8 – “A previous SIGINT assessment report on radicalization indicated that radicalizers...”

Anexo 9 – “Private Networks are Important”

Anexo 10 – Olympia & the case study

Anexo 11 – Boundless Informant

Anexo 12 – Chinese Exfiltrate Sensitive Military Technology

Anexo 13 – Intelligently filtering your data: Brazil and Mexico case studies

SUMÁRIO

INTRODUÇÃO	16
METODOLOGIA DE PESQUISA E DE REDAÇÃO DA TESE	26
I Complexidades da pesquisa sobre inteligência de Estado	26
II Parâmetros conceituais	30
III Limites materiais da tese	32
IV Hipóteses sugeridas	34
V Referenciais teóricos e premissas metodológicas	35
VI Alguns comentários sobre a técnica de redação da tese	41
VII Algumas notas sobre códigos utilizados em documentos classificados	42
1 A ATIVIDADE DE INTELIGÊNCIA ESTATAL	43
1.1 O que é e para que serve a inteligência de Estado	43
1.2 Como os Estados realizam inteligência?	44
1.2.1 O processo de requisição de autoridades por informações	45
1.2.2 A atividade de coleta de informações	47
a) Inteligência de fontes humanas (<i>Human-Source Intelligence – HUMINT</i>)	47
b) Inteligência de Sinais (<i>Signals Intelligence – SIGINT</i>)	50
c) Inteligência de Imagens (<i>Imagery Intelligence – IMINT</i>):	54
d) Inteligência de fontes abertas (<i>Open-Source Intelligence – OSINT</i>)	55
e) Inteligência de Mensuração e Assinaturas (<i>Measure and Signature Intelligence – MASINT</i>)	57
f) Inteligência Geoespacial (<i>Geospatial Intelligence – GEOINT</i>)	57
1.2.3 O processamento e a avaliação da informação	58
1.2.4 A atividade de análise de informações	60
1.2.5 A atividade de disseminação de informações	65
1.3 Como a atividade de inteligência é organizada	72
i. Office of the Director of National Intelligence (ODNI)	73
ii. Central Intelligence Agency (CIA)	73
iii. Defense Intelligence Agency (DIA)	74
iv. National Security Agency (NSA)	75
v. Federal Bureau of Investigation (FBI) – Intelligence Branch	75
vi. National Geospatial-Intelligence Agency (NGA)	75
vii. National Reconnaissance Office (NRO)	75

viii.	<i>Department of Energy (DOE) – Office of Intelligence and Counterintelligence.....</i>	76
ix.	<i>Department of Homeland Security (DHS) – Office of Intelligence and Analysis.....</i>	76
x.	<i>Department of State (DOS) – Bureau of Intelligence and Research</i>	76
xi.	<i>Department of Treasury (DOT) – Office of Intelligence and Analysis.....</i>	76
xii.	<i>Outras agências</i>	77
1.3.1	<i>Alguns apontamentos sobre a organização da inteligência brasileira</i>	77
1.4	Como a atividade de inteligência é fiscalizada.....	80
1.4.1	<i>Fiscalização interna.....</i>	81
1.4.2	<i>Fiscalização parlamentar</i>	82
1.4.3	<i>Fiscalização pelo executivo.....</i>	83
1.4.4	<i>Fiscalização pelo judiciário.....</i>	85
1.4.5	<i>Fiscalização por atores internacionais</i>	86
2	O ATUAL CONTEXTO POLÍTICO DO EXERCÍCIO DA INTELIGÊNCIA DE ESTADO – A RETÓRICA DA SEGURANÇA NA ERA DO MEDO	88
2.1	O impacto político-jurídico dos ataques de 11 de setembro de 2001.....	88
2.2	Percepção de ataques terroristas como resultado de falhas de inteligência.....	96
3	CAPACIDADES E EFEITOS COLATERAIS DE ESTRATÉGIAS ABRANGENTES DE INTELIGÊNCIA	102
3.1	Coleta de informações privadas de particulares.....	103
3.2	Espionagem econômica	112
3.3	Espionagem de informações classificadas	117
4	ANALISANDO A LICITUDE DAS ATIVIDADES DE ESPIONAGEM NO DIREITO INTERNACIONAL	129
4.1	A definição do conceito de espionagem.....	130
4.2	Os problemas de se posicionar a análise da licitude da espionagem sobre a dicotomia “guerra-paz”	133
4.3	A discussão sobre a licitude da espionagem de informações privadas de particulares.....	137
4.3.1	<i>A proteção internacional do direito humano à privacidade</i>	137
4.3.2	<i>Atritos entre privacidade e segurança: uma análise dos argumentos favoráveis à vigilância em massa.....</i>	150
4.3.2.1	<i>A falácia do argumento “Quem não deve não teme”</i>	151

4.3.2.2	Os problemas em se relacionar “privacidade” e “segurança” sob uma ideia de balanceamento	154
4.4	A discussão sobre a licitude da espionagem econômica	164
4.4.1	<i>A natureza concorrencial do segredo de empresa e sua categorização como espécie de propriedade intelectual</i>	<i>165</i>
4.4.2	<i>O vínculo entre Propriedade Intelectual e Comércio Internacional</i>	<i>167</i>
4.4.3	<i>A proteção da informação confidencial no acordo TRIPS e as atividades de espionagem econômica no contexto do comércio internacional</i>	<i>169</i>
4.4.4	<i>O argumento da “soberania econômica”</i>	<i>173</i>
4.5	A discussão sobre a licitude da espionagem de segredos de Estado	178
4.5.1	<i>A licitude dos atos de espionagem sob a “abordagem Lotus” e o formalismo no Direito Internacional</i>	<i>180</i>
4.5.2	<i>A licitude dos atos de espionagem por aplicação dos princípios gerais de direito.....</i>	<i>190</i>
4.5.2.1	<i>O argumento da ilicitude da espionagem pelo princípio da soberania e dos princípios corolários da não-intervenção e da integridade territorial</i>	<i>195</i>
4.5.3	<i>O argumento da licitude da espionagem por exercício do direito à legítima defesa... ..</i>	<i>206</i>
4.6	A escassez de parâmetros normativos como evidência da tolerância jurídica da espionagem internacional	210
5	UMA LEITURA REALISTA DAS CAUSAS DA TOLERÂNCIA DA ESPIONAGEM INTERNACIONAL	215
5.1	Revisitando o realismo político através dos estereótipos da crítica... ..	216
5.1.1	<i>Edward Hallet Carr</i>	<i>225</i>
5.1.2	<i>Hans Joachim Morgenthau</i>	<i>231</i>
5.1.3	<i>John Herz</i>	<i>237</i>
5.2	Análise realista das possibilidades regulatórias da espionagem internacional	240
5.2.1	<i>Alto custo de eventual fracasso das negociações.....</i>	<i>243</i>
5.2.2	<i>Limitações à promoção da segurança e ao poder</i>	<i>245</i>
5.2.3	<i>Dificuldades de fiscalização</i>	<i>256</i>
5.3	Conclusões provisórias: é necessário romper com ambiente de tolerância?	258
6	EFEITOS DO AMBIENTE DE TOLERÂNCIA DA ESPIONAGEM INTERNACIONAL DE SEGREDOS DE ESTADO E MECANISMOS DE INTERFERÊNCIA	262

6.1	A tolerância da espionagem internacional como artifício de conservação do <i>status quo</i>	263
6.2	A tolerância da espionagem internacional de segredos de Estado como atenuante do nível de incerteza no dilema da segurança	266
6.2.1	<i>Espionagem e mecanismos formais de verificação</i>	272
6.3	Redes de compartilhamento de informações como mecanismo de interferência no ambiente de tolerância	277
7	CONCLUSÃO	284
	REFERÊNCIAS	288

INTRODUÇÃO

"Let's be honest, we eavesdrop too. Everyone is listening to everyone else. But we don't have the same means as the United States, which makes us jealous".¹

(Bernard Kouchner, Ministro das Relações Exteriores da França no período de 2007 a 2010 e cofundador da organização Médicos sem Fronteiras).

Espionagem sempre foi um tabu nas relações internacionais. Pouco se discute sobre a prática em nível oficial e nunca houve qualquer iniciativa coordenada dos Estados voltada à sua regulamentação.² Como toda espécie de atividade clandestina³, a espionagem é envolvida por um ambiente marcado por alto grau de confidencialidade e fortemente influenciado pela retórica política dos Estados.

Esse efeito normalmente se manifesta em declarações de líderes estatais nas quais, diante de revelações de que seu Estado fora alvo de espionagem estrangeira, protestam com a genérica acusação de “violação de soberania”. O fez a ex-presidente Dilma Rousseff na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas⁴, ao exigir explicações do governo dos Estados Unidos sobre revelações de que a Agência de Segurança Nacional norte-americana – *National Security Agency (NSA)* – havia monitorado suas conversas telefônicas com seus

¹ HINNANT, Lori; DAHLBURG, John-Thor. 'Let's be honest, we eavesdrop too': former French foreign minister on NSA spying claims. **CTV News**, 23 out. 2013. Disponível em: <<http://www.ctvnews.ca/sci-tech/let-s-be-honest-we-eavesdrop-too-former-french-foreign-minister-on-nsa-spying-claims-1.1509912>>

² O que há são acordos secretos que dispõem sobre compartilhamento de informações entre Estados aliados. Um exemplo seria o *UKUSA Agreement*, acordo ajustado entre o Reino Unido e os Estados Unidos em 1946 como resultado da cooperação na área de inteligência durante a segunda guerra mundial, e que posteriormente se converteu em uma rede de compartilhamento de informações com a adesão do Canadá, Austrália e Nova Zelândia, formando o grupo conhecido como *Five Eyes*. Os documentos originais referentes ao acordo foram desclassificados no ano de 2010 e podem ser acessados em: NATIONAL SECURITY AGENCY. **UKUSA Agreement Release 1940-1956**. Disponível em: <https://www.nsa.gov/public_info/declass/ukusa.shtml>

³ Vale observar que, semanticamente, o vocábulo “clandestinidade” é a qualidade do que é oculto, escondido, não guardando qualquer relação com a ideia de “ilicitude” ou de “ilegalidade”. Portanto, a utilização da expressão no texto não sugere qualquer juízo de licitude.

⁴ “Estamos, Senhor Presidente, diante de um caso grave de violação dos direitos humanos e das liberdades civis; da invasão e captura de informações sigilosas relativas a atividades empresariais e, sobretudo, de desrespeito à soberania nacional. Fizemos saber ao Governo norte-americano nosso protesto, exigindo explicações, desculpas e garantias de que tais procedimentos não se repetirão” BRASIL. **Discurso de S.E. a Senhora Dilma Rousseff, Presidenta (sic) da República Federativa Do Brasil, na Abertura do Debate Geral da 68ª Sessão da Assembleia Geral das Nações Unidas**, Nova York, 24 set. 2013. Disponível em: <<http://www.onu.org.br/img/2013/09/Brasil-UNGA.pdf>>

principais assessores.⁵ Novos vazamentos de documentos altamente secretos da NSA continham menções à petroleira estatal *Petrobras*, o que sugeria indícios de espionagem econômica⁶, agravando assim a irresignação do governo brasileiro. Isso culminou com o cancelamento de visita de Estado aos Estados Unidos designada para o dia 23 de outubro de 2013. Especula-se ainda que as revelações de espionagem tenham prejudicado a posição da empresa *Boeing*, norte-americana fabricante do caça F/A-18, perante as concorrentes *SAAB*, sueca fabricante do caça *Gripen*, e *Dassault*, francesa fabricante do caça *Rafale*, em demanda do governo brasileiro pela compra de 36 aeronaves.⁷

Ainda no atribulado outubro de 2013, ao descobrir que suas comunicações eram alvo da vigilância da inteligência norte-americana⁸, a chanceler alemã Angela Merkel dirigiu veementes protestos a Barack Obama em conversa por telefone. Ao afirmar que a espionagem entre aliados é inadmissível, a chanceler foi publicamente apoiada por outros líderes europeus.⁹ A crise diplomática se agravou quando em 2014 a agência de inteligência alemã *Bundesnachrichtendienst (BND)* identificou entre seu pessoal um “agente duplo” que trabalhava em conjunto com a *Central*

⁵ Tal revelação foi originalmente divulgada na imprensa brasileira com base no conteúdo dos documentos vazados por Edward Snowden e por intermédio do jornalista Glenn Greenwald, então a serviço do *The Guardian*. Os documentos, classificados como altamente secretos (*Top Secret*), podem ser lidos em: VEJA os documentos ultrassecretos que comprovam espionagem a Dilma. **Fantástico**, 02 set. 2013. Disponível em: <<http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html>>

⁶ As suspeitas de que a espionagem a que foi submetida a Petrobras tenha finalidade comercial e estratégica foi agravada em razão da proximidade do leilão, designado para o dia 21 de outubro do mesmo ano de 2013, da concessão para exploração do “Campo de Libra”, região do mar territorial brasileiro que abarca o maior volume de “petróleo pré-sal” já descoberto. Cf. PETROBRAS foi espionada pelos EUA, apontam documentos da NSA. **Fantástico**, 08 set. 2013. Disponível em: <<http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html>>

⁷ WINTER, Brian. ENFOQUE - Como a espionagem dos EUA custou à Boeing um contrato multibilionário. **Reuters Brasil**, 20 dez. 2013. Disponível em: <<http://br.reuters.com/article/domesticNews/idBRSPE9BJ07Y20131220>>. O governo brasileiro decidiu pela compra de 36 jatos Gripen, da sueca SAAB, no valor total de 39,3 Bilhões de coroas suecas, o que equivale a cerca de 5,4 Bilhões de dólares. Cf. SILVEIRA, Virgínia. Governo brasileiro assina contrato da compra de 36 caças suecos Gripen. **Valor Econômico**, 27 out. 2014. Disponível em: <<http://www.valor.com.br/empresas/3750194/governo-brasileiro-assina-contrato-da-compra-de-36-cacas-suecos-gripen>>

⁸ Documentos classificados demonstraram que a NSA monitorou 200 números de telefone relacionados a 35 líderes mundiais, incluindo a chanceler alemã. Cf. BALL, James. NSA monitored calls of 35 world leaders after US official handed over contacts. **The Guardian**, 25 out. 2013. Disponível em: <<http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>>

⁹ 'THAT'S Just Not Done': Merkel Comments on Spying Allegations. **Spiegel Online International**, 24 out. 2013. Disponível em: <<http://www.spiegel.de/international/germany/merkel-comments-on-allegations-the-us-spied-on-her-cell-phone-a-929870.html>>

Intelligence Agency (CIA).¹⁰ Em represália, a Alemanha solicitou que o representante da CIA lotado na embaixada estadunidense em Berlim deixasse o país.¹¹

Mas no universo da política internacional passam efêmeros os ressentimentos se os benefícios em tolerar a ofensa são maiores que os de resistir-lhe. Se em 2013 a presidente brasileira exigia desculpas do governo americano diante de uma entusiasmada assembleia geral da ONU, em menos de dois anos depois realizou a visita oficial aos Estados Unidos, antes cancelada sob veementes protestos. Nessa nova oportunidade, uma amistosa comitiva brasileira não exigiu qualquer pedido de desculpas, afirmando a ex-presidente Dilma Rousseff que “O Presidente Obama e o governo dos Estados Unidos declararam, em várias oportunidades, que eles não iriam mais cometer atos intrusivos de espionagem sobre países amigos. Eu acredito no Presidente Obama”.¹² ¹³ Ocorre que o ex-Presidente Obama nunca fez essa declaração. Por fim, todas as propostas levantadas pelo governo brasileiro de se criar serviços nacionais independentes de *internet* e armazenamento de informações nunca se realizaram e a reação à espionagem parece mesmo ter se resumido a enunciados de proteção da privacidade no “Marco Civil da Internet”, aprovado em 2014 (Lei 12.965).

Os protestos do governo alemão também se silenciaram diante de revelações de que o *BND* cooperou com a *NSA* em atividades de espionagem com alvos europeus. O consórcio, de codinome EIKONAL, foi exposto pelo parlamentar austríaco Peter Pilz e supostamente teria possibilitado que fossem espionadas

¹⁰ KNIGHT, Ben. Germany reacts to 'double agent' scandal. **DW**, 07 jul. 2014. Disponível em: <<http://dw.com/p/1CXmf>>

¹¹ OLTERMANN, Philip. ACKERMAN, Spencer. Germany asks top US intelligence official to leave country over spy row. **The Guardian**, 10 jul. 2014. Disponível em: <<http://www.theguardian.com/world/2014/jul/10/germany-asks-top-us-intelligence-official-spy-row>>

¹² “President Obama and the US government have stated on several occasions that they would no longer engage in intrusive acts of spying on friendly countries. I believe President Obama”. ROBERTS, Dan. Brazilian president's visit to US will not include apology from Obama for spying. **The Guardian**, 30 jun. 2015. Disponível em: <<http://www.theguardian.com/world/2015/jun/30/brazil-dilma-rousseff-obama-nsa-spying-apology>>

¹³ As razões da “mudança de tom” do governo brasileiro em relação à espionagem americana podem ser explicadas pelo posterior enfraquecimento político da Presidente Dilma Rousseff – que viu sua taxa de aprovação decair para patamares de um dígito – e econômico do país, que se encontrava em recessão. Nesse cenário de turbulência, tentativas de reconciliação com aliados tradicionais e de evitar posições que pudessem causar qualquer tipo de atrito externamente contribuiriam para um ambiente de maior tranquilidade, desejável pelo governo brasileiro. Cf. BEVINS, Vincent. Why did Brazil's President Change Her Tune on Spying? **Foreign Policy**, 16 jun. 2015. Disponível em: <<http://foreignpolicy.com/2015/06/16/brazil-nsa-spying-surveillance-economy-dilma-rousseff-barack-obama/>>

grandes companhias de telecomunicações europeias, dentre elas a *Swisscom*¹⁴ e a *Belgacom*¹⁵, entre os anos de 2005 e 2008. As denúncias motivaram o início de investigações oficiais junto à procuradoria-geral da Suíça, da Bélgica, da Holanda¹⁶ e da Áustria.¹⁷

Por outro lado os Estados Unidos também têm suas próprias razões para se preocupar com atividades de espionagem de um Estado estrangeiro.¹⁸ Poucos meses antes das revelações de Edward Snowden, o executivo estadunidense publicou o estudo “*Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*” (Estratégia da Administração na Mitigação da Subtração de Segredos Comerciais dos Estados Unidos).¹⁹ Uma extensa lista de casos criminais que envolveram obtenção ilícita de segredo de empresa por chineses em companhias privadas (por exemplo: *Dupont, General Motors, Ford, Cargill*) e setores do governo dos Estados Unidos integra o documento.²⁰

Evidências mais concretas permitiram associar a origem de atos de ataque cibernético ao território chinês. Uma companhia privada de segurança cibernética norte-americana, *Mandiant*, por conseguir rastrear a fonte de atividades de espionagem cibernética com alvo nos Estados Unidos até instalações militares do Exército de Libertação Popular em Xangai (especificamente na “unidade 61398” - 61398部队), apresentou em relatório dados consistentes que permitiram concluir que o governo chinês conduz programas de espionagem econômica.²¹ Setores estratégicos da economia norte-americana foram, segundo o relatório, alvos da

¹⁴ ALLEN, Ian. Switzerland to probe claims it was spied on by US, German agencies. **Intelnews.org**, 28 maio 2015. Disponível em: <<http://intelnews.org/2015/05/28/01-1705/>>

¹⁵ *Idem*. Belgium launches official probe into alleged German-US espionage. **Intelnews.org**, 8 jun. 2015. Disponível em: <<http://intelnews.org/2015/06/08/01-1710/>>

¹⁶ *Ibidem*.

¹⁷ GERMAN ‘Spying’ prompts Austria complaint. **BBC News**, 5 maio 2015. Disponível em: <<http://www.bbc.com/news/world-europe-32596510>>

¹⁸ O que se segue a respeito de espionagem econômica China-EUA foi objeto de publicações anteriores de nossa autoria, principalmente em: LIMA, Humberto Alves de Vasconcelos; CUNHA, Naiana Magrini Rodrigues. O problema da espionagem econômica internacional: seria a Organização Mundial do Comércio o foro adequado para sua apreciação? **Revista de Direito Internacional**, v. 12, n. 2, 2014. p. 92-106. Disponível em: <<http://www.publicacoesacademicas.uniceub.br/index.php/rdi/article/view/3017/pdf>>

¹⁹ EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES. **Administration Strategy on Mitigating The Theft of U.S. Trade Secrets**, fev. 2013. Disponível em: <https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>

²⁰ *Ibidem*. Cf. o anexo do documento: “*Summary of Department of Justice Economic Espionage and Trade Secret Criminal Cases*”.

²¹ MANDIANT. **APT1: Exposing One of China’s Cyber Espionage Units**, 2013. Disponível em: <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>

espionagem chinesa, especialmente dos ramos de tecnologia da informação e aeroespacial²² (cf. seção 3.2). O então Diretor da NSA, o General Keith Alexander, afirmou em 2012 que estes eventos representavam a maior transferência de riqueza da história.^{23 24}

Diante da massiva quantidade de evidências – em alguns casos provas diretas – da espionagem estatal chinesa, a reação do governo Obama para lidar com o problema evoluiu de medidas diplomáticas²⁵, para o campo jurídico, quando cinco oficiais do exército chinês foram acusados perante o judiciário dos Estados Unidos por atos de espionagem cibernética. Foi a primeira vez que agentes de Estado estrangeiros foram acusados perante cortes do país por esse tipo de conduta, segundo o então Procurador-Geral Eric Holder.²⁶ É fácil perceber que tais acusações guardam pretensões estritamente políticas²⁷, pois uma condenação criminal dependeria da cooperação do governo chinês na extradição dos indiciados,

²² *Ibidem.* p. 24.

²³ O General esclareceu que companhias norte-americanas perdem cerca de 250 bilhões de dólares por ano por subtração de propriedade intelectual, além de 114 bilhões perdidos anualmente com crimes cibernéticos. Cf. ROGIN, Josh. NSA Chief: Cybercrime constitutes the greatest transfer of wealth in history. **Foreign Policy**, 9 jul. 2012. Disponível em: <http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history>

²⁴ O rigor acadêmico aconselha a desconfiar da precisão dos valores que as indústrias e o governo alegam representar o prejuízo financeiro que suportam com a espionagem econômica. De fato, *“The ultimate value of economic secrets, unlike directly monetizable assets like bank accounts, depends not only on the cost of producing them but also on a firm’s ability to capitalize on the information in a competitive marketplace. The net value of lost market share, lost jobs, and the overhead of technical and legal defense is a very complicated equation”*. LINDSAY, Jon R.; CHEUNG, Tai Ming. From Exploitation to Innovation Acquisition, Absorption, and Application. In: LINDSAY, Jon R.; CHEUNG, Tai Ming; REVERON, Derek S. **China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain**. Oxford University Press, 2015. p. 52.

²⁵ Negociações diplomáticas sobre a questão da espionagem cibernética fracassaram em diálogos EUA-China, que aconteceram em meados do ano de 2013. Cf. ROBERTS, Dan; GOLDENBERG, Suzanne. US-China summit ends with accord on all but cyber-espionage. **The Guardian**, 10 jun. 2013. Disponível em: <<http://www.theguardian.com/world/2013/jun/09/us-china-summit-barack-obama-xi-jinping>>

²⁶ Os cinco oficiais chineses, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, e Gu Chunhui, foram indiciados por um Grand Jury do Distrito Oeste da Pensilvânia com acusações associadas à ciberspionagem econômica, direcionadas contra as empresas Westinghouse, SolarWorld, U.S. Steel, ATI, USW e Alcoa Inc. Cf. UNITED STATES DEPARTMENT OF JUSTICE. **U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage**, 19 maio 2014. Disponível em: <<http://www.justice.gov/opa/pr/2014/May/14-ag-528.html>>

²⁷ Uma interessante análise dos reais objetivos das acusações pode ser lida em: CHABROW, Eric. The Real Aim of the U.S. Indictment of Chinese. **Bank Info Security**, 20 maio 2014. Disponível em: <<http://www.bankinfosecurity.com/real-aim-us-indictment-chinese-a-6854/op-1>>

o que não se espera que ocorra tendo em vista que suas autoridades negam enfaticamente ter patrocinado atividades de espionagem.²⁸

Todos estes eventos servem para ilustrar a maneira contraditória com que líderes de Estado se manifestam oficialmente sobre atos de espionagem. Quando se descobrem alvo da inteligência clandestina de outro Estado externam suas queixas mais enfáticas; quando são revelados contumazes espiões, justificam a coleta de informações por estritas razões de segurança nacional. Como bem observou Simon Chesterman:

Isso se deve em parte à forma irreflexiva de que governos abordam o assunto: nós e nossos amigos simplesmente coletamos informação; você e seu tipo violam soberania. A maioria dos sistemas jurídicos então busca proibir a coleta de inteligência por agentes estrangeiros enquanto protegem a capacidade do próprio Estado de conduzir tais atividades externamente.²⁹

A bem da verdade, não é razoável exigir que um governo se pronuncie de forma absolutamente transparente e aberta acerca das capacidades e atividades dos serviços de inteligência de seu Estado. É da natureza da inteligência a confidencialidade, sem a qual pode-se comprometer seu próprio objeto que é a obtenção da informação. Além disso, se um Estado possui o interesse concomitante em proteger seus segredos e obter segredos de outros, é de se esperar que sua legislação coíba a espionagem interna e fomenta a externa – conclusão que, apesar da obviedade, não legitima, por si só, a disparidade. Esse “efeito irreflexivo”, adotando a expressão empregada por Simon Chesterman, foi reconhecido por Barack Obama em discurso na NSA:

[...] as garantias legais que restringem a vigilância contra pessoas nos Estados Unidos sem um mandado judicial não se aplicam a

²⁸ Não obstante, em visita de Estado do Presidente chinês Xi Jinping aos Estados Unidos em setembro de 2015, as duas partes se comprometeram a não realizar atividades de espionagem econômica e a manter diálogos entre oficiais de alto escalão com atribuições para verificar alegações de intrusão cibernética. Cf. NAKASHIMA, Ellen; MUFSON, Steven. The U.S. and China agree not to conduct economic espionage in cyberspace. **The Washington Post**, 25 set. 2015. Disponível em: <https://www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html?tid=sm_fb>

²⁹ “This is due in part to the nonreflexive manner in which governments approach the subject: we and our friends merely gather information; you and your type violate sovereignty. Most domestic legal systems thus seek to prohibit intelligence gathering by foreign agents while protecting the state’s own capacity to conduct such activities abroad”. CHESTERMAN, Simon. The Spy Who Came in From the Cold War: Intelligence and International Law. **Michigan Journal of International Law**, v. 27, 2006. p. 1072.

estrangeiros no exterior. Isso não é único da América; poucas, se há, agências de espionagem ao redor do mundo limitam suas atividades além de suas fronteiras. E inteligência é tudo sobre obter informação que não está publicamente disponível. Mas as capacidades da América são únicas, e o poder de novas tecnologias significam que existem cada vez menos restrições técnicas sobre o que nós podemos fazer. Isso coloca uma obrigação especial sobre nós de perguntar sobre o que nós devemos fazer. E finalmente, agências de inteligência não podem funcionar sem sigilo, o que faz com que seu trabalho seja menos sujeito ao debate público.³⁰

De fato, o tratamento díspare que um Estado confere às suas próprias atividades de espionagem com relação à espionagem estrangeira é compreensível do ponto de vista estratégico. Mas é também causa da mais grave insegurança sobre os limites jurídicos da espionagem internacional. Pois, se do ponto de vista da legislação doméstica de um Estado a espionagem interna é geralmente proscrita e a externa lícita, um Estado que se insurja denunciado a pretensa ilicitude de um ato de espionagem estrangeira da qual fora alvo, eventualmente se verá obrigado a justificar, em sentido contrário, a licitude de suas próprias atividades de mesma natureza.

É certo que a licitude no Direito Internacional não se confunde com a licitude no Direito Interno dos Estados, de sorte que um mesmo ato pode ser concomitantemente ilícito segundo o Direito Internacional e lícito de acordo com determinada legislação doméstica ou vice-versa.³¹ Mas no caso específico da espionagem, há grande dificuldade em se definir qual o exato *status* normativo da atividade segundo o Direito Internacional.

³⁰ *“Third, the legal safeguards that restrict surveillance against U.S. persons without a warrant do not apply to foreign persons overseas. This is not unique to America; few, if any, spy agencies around the world constrain their activities beyond their own borders. And the whole point of intelligence is to obtain information that is not publicly available. But America’s capabilities are unique, and the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do. And finally, intelligence agencies cannot function without secrecy, which makes their work less subject to public debate”*. TRANSCRIPT of President Obama’s Jan. 17 speech on NSA reforms. **The Washington Post**, 17 jan. 2014. Disponível em: <http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html>

³¹ Trata-se de uma noção já sólida na doutrina da responsabilidade internacional dos Estados. O Artigo 3º do “Projeto da Comissão de Direito Internacional da Organização das Nações Unidas sobre Responsabilidade de Estados” determina que: “A caracterização de um ato de um Estado como internacionalmente ilícito é regida pelo Direito Internacional. Tal caracterização não é afetada pela caracterização do mesmo ato como lícito pelo direito interno”. Um detalhado histórico da observância a esse princípio em decisões de cortes internacionais pode ser lido em UNITED NATIONS. Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, **International Law Commission**, 2001. p. 36-38. Disponível em: <http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>

Não há dúvidas de que a coleta de informações não confidenciais – isto é, a atividade ordinária de inteligência – é perfeitamente lícita no Direito Internacional. Mesmo não havendo expressa menção a isso em tratado, a licitude da atividade pode ser inferida do fato de que a maior parte dos Estados nela se engaja e nenhum contra ela protesta. Diante de um padrão de comportamento estatal uniforme e aceito como sendo juridicamente compatível, pode-se concluir estar-se diante de uma prática consolidada como costume internacional. Além disso, algumas normas convencionais parecem reconhecer indiretamente a licitude da coleta de informações não confidenciais. Tome-se como exemplo disposições da Convenção de Viena sobre Relações Diplomáticas de 1961, que incluem entre as funções da missão diplomática a de “inteirar-se por todos os meios lícitos das condições existentes e da evolução dos acontecimentos no Estado acreditado e informar a esse respeito o Governo do Estado acreditante” (art. 3); bem como as garantias de livre comunicação da missão com seu governo e de inviolabilidade dos arquivos, documentos, correspondências e da mala diplomática da missão (art. 24 e 27). Além disso, autoriza-se ao Estado acreditante o envio de adidos das forças militares, navais ou aéreas (art. 7), presumivelmente para exercer funções de inteligência.³²

Todavia, tratando-se de atividades de obtenção de informações classificadas ou de outra forma mantidas em segredo por um Estado – ou seja, espionagem – a licitude da prática é questionável e desperta séria insegurança, ao menos no que diz respeito à sua ocorrência em tempo de paz.³³ Tal dificuldade se origina do fato de não existir qualquer proibição expressa às atividades de espionagem em tratado internacional ou mesmo não se possa extrair qualquer conclusão normativa a respeito dessa prática através do costume internacional.

As duas principais constatações que foram apresentadas até o momento, isto é, a maneira irreflexiva com que Estados abordam politicamente a questão da espionagem e a insegurança quanto a licitude da atividade perante o Direito Internacional sugerem um ambiente de tolerância jurídica e política da atividade, o que constitui a problemática inicial da tese. **Nesse contexto, a pesquisa é orientada a aferir a real existência desse ambiente de tolerância jurídico-**

³² CHESTERMAN, S. *op. cit.* p. 1087.

³³ No contexto de um conflito armado internacional a espionagem é, inequivocamente, lícita de acordo com o Direito Internacional. Tal condição será explicada na seção 4.2.

política da espionagem internacional e, em caso positivo, compreender suas causas, o seu significado e suas consequências.

Inicialmente, superadas considerações metodológicas a que se dedica a seção seguinte, é feito no capítulo 1 um estudo propedêutico e descritivo sobre a atividade de inteligência estatal, onde são examinadas suas atribuições, sua estrutura e funcionamento, bem como os mecanismos de controle e fiscalização correspondentes. A isso é adicionada, no capítulo 2, uma análise do contexto político atual sobre o qual operam alguns dos principais serviços de inteligência do mundo, argumentando-se que a retórica da segurança diante de ameaças terroristas do extremismo islâmico foi o principal fator que os impulsionou. No capítulo 3 são discutidos os principais problemas associados a uma estratégia abrangente de inteligência de Estado.

A partir daí a tese passa de uma abordagem descritiva para um estudo teórico crítico de Direito Internacional e Relações Internacionais. No capítulo 4, assume-se postura dogmática para oferecer resposta ao problema da licitude da espionagem internacional em tempo de paz. Nessa análise o problema é estratificado para que se possa examinar criticamente a licitude de diferentes modalidades de espionagem segundo o Direito Internacional, sugerindo-se a seguinte e inédita classificação: a) informações privadas de particulares; b) segredos de empresa e c) segredos de Estado. Tal estratificação é uma proposição central da tese e se justifica em razão da diferença de natureza do titular da informação – respectivamente particulares, empresas e Estados – bem assim dos tipos de informação e dos correspondentes regimes normativos de Direito Internacional em que se inserem: a proteção internacional dos direitos humanos, a proteção internacional da propriedade intelectual, e a proteção da soberania nacional. Desse modo, pretende-se verificar se a espionagem internacional viola cada uma dessas formas de tutela quando têm por objeto os diferentes tipos de informação mencionados. As constatações ali alcançadas são sintetizadas na conclusão de que a escassez de normas de Direito Internacional aplicáveis ao problema da espionagem determina um ambiente de tolerância da atividade, mas que se manifesta em diferentes graus de acordo com a modalidade da atividade.

No capítulo 5 é realizado um estudo das causas da tolerância da espionagem internacional sob as proposições do realismo político, ou seja, dos fatores que desacreditam pretensões de regulação da atividade no Direito Internacional e fazem

perpetuar a maneira lacunosa com que é ela tratada politicamente. Isso é precedido de uma proposta de revisitação do realismo político através da reavaliação das próprias críticas que a ele são dirigidas.

Por fim, no capítulo 6, são investigados, também sob o prisma realista, o significado político e as consequências que um ambiente de tolerância da espionagem produz nas relações internacionais.

METODOLOGIA DE PESQUISA E DE REDAÇÃO DA TESE

“One of the important differences between academe and the intelligence community is that in most universities one has the right to be wrong. Universities are built upon making mistakes; there could be no valid research were there not hundreds of feints, aborted projects, invalid conclusions. And one must not be punished, or intimidated, for mistakes honestly made. No government bureaucracy could hold to such a principle.”³⁴
(Robin W. Winks).

I Complexidades da pesquisa sobre inteligência de Estado

Realizar pesquisas acadêmicas na temática da inteligência de Estado é uma tarefa que acarreta complexidades adicionais em relação às investigações de outros assuntos. Inicialmente, há dificuldades em se obter acesso a fontes primárias em razão da confidencialidade que envolve a atividade. A maior parte das operações de agências de inteligência são classificadas bem como toda documentação oficial pertinente, havendo severas penalidades para a divulgação indevida de informações dessa qualidade. Com exceção de poucos acadêmicos privilegiados a quem é concedido acesso interno à documentação classificada (como, por exemplo, historiadores oficiais a serviço do governo), os demais pesquisadores se verão desafiados a conduzir sua investigação com recursos bastante limitados. “Inteligência, pois, por definição, resiste ao estudo acadêmico”³⁵, como afirmou Michael Warner.

Não bastasse as dificuldades que a confidencialidade acarreta para o estudo da inteligência de Estado, tal tarefa se revela mais desmotivadora diante das exigências da comunidade acadêmica. A maioria das universidades, especialmente nos Estados Unidos, Canadá e Europa, condiciona a contratação e estabilidade no cargo de professor a grande número de publicações em períodos relativamente

³⁴ WINKS, Robin W. **Cloak and Gown**: Scholars in the Secret War, 1939–1961. New York: William Morrow, 1987.

³⁵ “*Intelligence thus by definition resists scholarship*”. WARNER, Michael. Sources and methods for the study of intelligence In JOHNSON, Lock K. (org.) **Handbook of Intelligence Studies**, London: Routledge, 2007. p. 17.

curtos de tempo.³⁶ “*Publish or perish!*”. Isso cria, como destaca Amy Zegart, fortes incentivos para que acadêmicos pesquisem tópicos com dados que estão facilmente disponíveis, de sorte que as publicações possam ser alcançadas mais rapidamente.³⁷

Sintomaticamente, o estudo acadêmico da inteligência é ainda incipiente, apesar de crescente.³⁸ Não se trata de uma temática que atingiu profundidade de estudo filosófico, ou mesmo uma sistematização teórica clara e precisa. Por essa razão, a literatura sobre inteligência é fragmentada e a maior parte dos estudos foram publicados na forma de artigos científicos, sendo relativamente baixo o número de livros.

Nos Estados Unidos e Reino Unido se concentra o maior número de pesquisadores na área, naturalmente em razão da expertise reunida com a atividade durante a segunda guerra mundial e impulsionada no período da guerra fria. Autores de densas obras sobre inteligência de Estado podem lá ser encontrados, a exemplo dos historiadores Matthew Aid, Sherman Kent (1903-1986), John Keegan (1934-2012) e o historiador oficial britânico para a Segunda Guerra Mundial, Sir Francis Harry Hinsley (1918-1998), do cientista político Lock K. Johnson, Michael Herman, entre outros importantes nomes. No Brasil é preciso reconhecer os estudos em inteligência de Estado de Marco Aurélio Cepik, atualmente Professor de Ciências Políticas na Universidade Federal do Rio Grande do Sul.

Não obstante as complexidades que envolvem o estudo da inteligência que foram mencionadas anteriormente, existem meios de acesso a fontes primárias que atenuam essa condição. Um desses meios é o mecanismo de desclassificação previsto na legislação, que define prazos específicos para a manutenção do sigilo da informação de acordo com o nível de classificação, ao fim dos quais a informação passa ao domínio público. Por exemplo, no Brasil, a chamada “Lei de Acesso à Informação” (Lei 12.527/2011) define, em seu artigo 24, §1º, que o prazo máximo de

³⁶ Trata-se da figura da “*Tenure*”, um direito contratual conferido a professores que, após um período probatório e a satisfação de rigorosas exigências acadêmicas, não mais podem ser demitidos sem que haja justa causa para tanto.

³⁷ ZEGART, Amy B. Cloaks, Daggers, and Ivory Towers: Why Academics Don't Study U.S. Intelligence. In JOHNSON, Lock K. (org.) **Strategic Intelligence**, v. 1, Preager Security International, 2007. p. 27.

³⁸ Em 2016 recebemos com satisfação a notícia de que a edição anual da *Philip C. Jessup International Law Moot Court Competition* abordaria a licitude de programas de vigilância em massa e as consequências jurídicas de Direito Internacional para ataques cibernéticos. A equipe da Faculdade de Direito da UFMG – que tivemos a oportunidade de auxiliar em algumas ocasiões – venceu a etapa nacional da competição e fez ótima participação na fase internacional.

restrição da informação ultrassecreta é de 25 anos, da secreta 15 anos e da reservada 5 anos, todos contados a partir da data da produção da informação. Findo o prazo, a informação automaticamente se torna “de acesso público” (§ 4º). Nos Estados Unidos, através do *website* da *Central Intelligence Agency* (CIA), pode-se pesquisar extenso número de documentos desclassificados através do *Freedom of Information Act* (FOIA).³⁹

Paralelamente, há um número crescente de documentos classificados que são “vazados”⁴⁰ para a imprensa pelos chamados *whistleblowers*⁴¹, que – abstraindo-se do fato de que são divulgados ilicitamente⁴² – fornecem valiosas fontes para a pesquisa por se tratarem de informações até então sigilosas. Isso significa que possibilitam análises mais atualizadas sobre os serviços de inteligência, em contraste com informações regularmente desclassificadas que, em razão do longo prazo de manutenção do sigilo, especialmente em relação às informações altamente secretas, muitas vezes nos chegam ao conhecimento em descompasso com a realidade atual. Logo, tanto as informações regularmente desclassificadas

³⁹ Cf. CENTRAL INTELLIGENCE AGENCY. **Freedom of Information Act Electronic Reading Room**. Disponível em: <<http://www.foia.cia.gov/>>

⁴⁰ A expressão vem do inglês “*leak*” (“vazamento”), que é comumente empregada na imprensa para descrever o desvio e divulgação de informações confidenciais.

⁴¹ A tradução literal seria “sopradores de apito”. O termo alude à figura do árbitro desportivo que sopra o apito para indicar uma ação irregular de um jogador, e foi cunhado para designar indivíduos que denunciasses más condutas governamentais, evitando assim outras expressões pejorativas como “informante” ou “delator”. Cf. NADER, Ralph; PETKAS, Peter J.; BLACKWELL, Kate (org.) **Whistle Blowing: the report on the conference on professional responsibility**. Grossman Publishers, 1972.

⁴² Como o acesso que os *whistleblowers* possuem é autorizado com base em uma relação especial de confiança, o vazamento de documentos classificados constitui crime federal nos Estados Unidos, punido no *Espionage Act* de 1917 sob a epígrafe “*Disclosure of Classified Information*” (18 U.S. Code § 798). Já o veículo de imprensa que divulga os documentos, argumenta-se, estaria resguardado pela Primeira Emenda à Constituição dos Estados Unidos, que garante a liberdade de expressão e de imprensa. Há quem argumente que as garantias da Primeira Emenda devem se estender também ao responsável pelo vazamento da informação classificada. Cf. KITROSSER, Heidi. Free Speech aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information. **Journal of National Security Law & Policy**, v. 6, p. 2013. Vale notar que a utilização de documentos vazados, publicados através do portal *Wikileaks*, tem sido aceita até mesmo em julgamentos de cortes internacionais como nos casos *Prosecutor v. Charles Ghankay Taylor* perante a Corte Especial para Serra Leoa e *Prosecutor v. Salim Jamil Ayyash et. al.* – *Admissibility of documents published on the Wikileaks website*, 21 maio 2015, do Tribunal Especial para o Líbano. Por tudo isso, devem preocupar notícias tais como a de uma candidata ao *PhD* da *Antioch University* que foi forçada a retirar de sua tese de doutoramento todas as referências a documentos publicados pelo *Wikileaks*, sob pena de não ver seu trabalho publicado – uma exigência para obtenção do título no caso. Cf. CUTHBERTSON, Anthony. PhD student forced to remove all WikiLeaks references from her dissertation. **International Business Times**, 10 set. 2015. Disponível em: <<http://www.ibtimes.co.uk/phd-student-forced-remove-all-wikileaks-references-her-dissertation-1519172>>

quanto as informações “vazadas” permitem ao pesquisador acesso às fontes primárias da pesquisa sobre inteligência estatal.

Deve-se acautelar o pesquisador, no entanto, que essa forma de acesso às fontes primárias apenas revela uma parcela bem pequena do emaranhado de documentos em que se formalizam tanto as operações quanto o produto dos serviços de inteligência, de sorte que qualquer análise que a partir delas se construa fornecerá um panorama inevitavelmente fragmentado. A isso o pesquisador deve responder, aconselha Michael Warner, com a cautela de “construir generalizações apenas sobre bases fáticas estáveis”.^{43 44}

Com efeito, a tese é construída sobre uma sólida base fática. Tratando-se de uma pesquisa de Direito Internacional e Relações Internacionais, há grande número de referências a pronunciamentos de autoridades estatais, a decisões de política internacional, a negociações diplomáticas, e outros fatos e eventos referentes à ação externa do Estado. Nesses casos, preferiu-se por buscar a informação em portais oficiais governamentais e na imprensa especializada, como por exemplo as revistas *Foreign Affairs*, *Foreign Policy*, *The Economist*, ou de jornalistas especializados em análise internacional de grandes veículos como *Washington Post*, *The New York Times*, *CNN*, *BBC*, *The Guardian*, *Der Spiegel*, alguns deles inclusive agraciados com o prêmio *Pulitzer*. Também se recorreu à mídia especializada de *websites* independentes como *Intelnews.org*, *Lawfare* e *Wikileaks*.

Um jornalista cujas reportagens e obra aparecem com frequência nas referências é o inglês radicado no Brasil Glenn Greenwald. Isso se explica pelo fato de ter sido ele o principal contato de Edward Snowden com a imprensa, ficando responsável, quando a serviço do jornal *The Guardian*, pela publicação dos documentos vazados. Suas reportagens, portanto, tratam-se das fontes mais diretas que se pode ter sobre estes documentos, tendo em vista sua natureza classificada.

⁴³ “He has to word his judgments accordingly, erring always on the side of caution, and building to generalizations only on stable bases of fact”. WARNER, M. *op. cit.* p. 21-22.

⁴⁴ Advertência que fez recordar lição de Bertrand Russel quando questionado, em entrevista à *BBC* em abril de 1959, sobre qual conselho gostaria de deixar para gerações futuras, respondeu: “[...] *The intellectual thing I should want to say to them is this: When you are studying any matter or considering any philosophy, ask yourself only what are the facts and what is the truth that the facts bear out. Never let yourself be diverted either by what you wish to believe or by what you think would have beneficent social effects if it were believed, but look only and solely at what are the facts. That is the intellectual thing that I should wish to say [...]*”. A entrevista pode ser assistida e sua transcrição lida em: http://www.openculture.com/2012/08/face_to_face_with_bertrand_russell_love_is_wise_hatred_is_foolish.html>

Para mitigar, ainda que pouco, o problema da dificuldade de obtenção de fontes primárias na pesquisa em inteligência de Estado, optou-se sempre por buscar a referência original na literatura quando for ela citada por terceiro, evitando-se assim a fórmula “*apud*”.

II Parâmetros conceituais

i. Inteligência

A expressão “inteligência” é basicamente empregada em três sentidos diversos na literatura e no jargão profissional da comunidade de inteligência. Fala-se em “inteligência” como sendo:

- a) as agências estatais de coleta e análise de informações (como na frase: “A *inteligência* dos Estados Unidos tem conhecimento da localização dos terroristas”);
- b) a atividade de coleta de informações (como na frase: “Na guerra fria a *inteligência* foi principalmente conduzida por oficiais infiltrados”);
- c) as informações obtidas e processadas através do serviço estatal de coleta e análise de informações (como na frase: “A *inteligência* que nos foi fornecida permite saber exatamente de onde se originam os ataques cibernéticos”).

Na tese, a expressão “inteligência” será utilizada exclusivamente no primeiro e no segundo sentido, isto é, as *agências* ou a própria *atividade* de coleta e análise de informações. No terceiro sentido, não se falará em “inteligência”, mas sim em “informação” ou “informações qualificadas pela inteligência” (*finished intelligence*), conforme o caso.

ii. Inteligência de Estado

Utiliza-se essa expressão na tese para designar a atividade de inteligência de mais alto nível de um Estado, organizada para informar líderes e outras autoridades de alto escalão.

É comum denominar o serviço de investigação para propósitos de persecução penal como “inteligência”. Na tese a expressão “inteligência de Estado” exclui de sua abrangência as atividades dessa natureza.

iii. Inteligência externa

Atividade de coleta de informação que está localizada em território estrangeiro.

iv. Espionagem

Atividade de inteligência clandestina, na qual se objetiva coletar, através de uma operação sigilosa, informação classificada ou de outra forma mantida em segredo. A elaboração desse conceito é feita na seção 4.1.

Por vezes se utilizará na tese a expressão “inteligência ordinária” para se distinguir da “inteligência clandestina”, que é a espionagem.

v. Espionagem econômica

Obtenção clandestina de informação cujo sigilo é protegido por lei e seu conhecimento é apto a proporcionar vantagem concorrencial ou econômica.

vi. Segredos de Estado

Informações estatais oficiais e sigilosas de natureza política ou militar.

vii. Vigilância

Coleta persistente de informações através da monitoração da fonte.

III Limites materiais da tese

Em essência, a tese tem por objeto o estudo das atividades de inteligência e espionagem, compreendidas como meras atividades de obtenção de informação, que não envolvem atos coercitivos.

Essa ressalva se justifica pois existem outros tipos de operações secretas frequentemente conduzidas por agências de inteligência, caracterizadas pelo fato de que são realizadas com o cuidado de não se poder associar sua prática ao Estado que a patrocina, exatamente por serem ilícitas, seja do ponto de vista do Direito Internacional – normalmente por violar o princípio da não-intervenção – ou mesmo do Direito Interno do local onde são realizadas. Conhecidas vulgarmente na literatura norte-americana como “*The Third Option*” – a terceira opção (entre o envio de *marines* ou de diplomatas), as “operações encobertas” (*covert operations; covert action; black operations*) podem consistir em assassinatos de líderes ou dissidentes políticos, auxílios a golpes de Estado⁴⁵, fornecimento de armas a grupos rebeldes, sabotagem, manutenção de prisões secretas em outros países, prática de tortura em interrogatórios, entre tantas outras. São normalmente conduzidas por agências de inteligência por reunirem elas a expertise necessária para que se possa sustentar com êxito o véu que separa o Estado da operação. Essas atividades não serão objeto da pesquisa.

Também não serão objeto da pesquisa operações de contra-inteligência, que consistem no conjunto de procedimentos utilizados para identificar, superar e neutralizar atividades de inteligência de um Estado ou organização estrangeiro.⁴⁶

Por se tratar de uma pesquisa do domínio do Direito Internacional e das Relações Internacionais, se limitará a investigar as atividades de inteligência e

⁴⁵ Oportuno lembrar, a propósito, que há pouco mais de 50 anos a CIA envidava esforços para pressionar a ocorrência do golpe militar de 1964 no Brasil, com presença de agentes no país conduzindo operações secretas de fomento a protestos de rua “pró-democracia” e “encorajamento de sentimentos democráticos e anticomunistas” no Congresso, Forças Armadas, grupos sindicais e estudantis, igreja e empresas, como relatado em documentos desclassificados. Paralelamente, a marinha estadunidense deslocou uma força tarefa naval do Caribe para a costa brasileira, em Santos, para suprir os golpistas com armamentos e suprimentos caso fosse necessário. Os documentos desclassificados e gravações de áudio que comprovam o envolvimento direto dos Estados Unidos no golpe de Estado podem ser acessados em THE NATIONAL SECURITY ARCHIVE. **Brazil Marks 40th Anniversary of Military Coup Declassified Documents Shed Light on U.S. Role.** Disponível em: <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB118/index.htm#docs>

⁴⁶ LERNER, K. Lee; LERNER, Brenda Wilmoth. (orgs.) **Encyclopedia of Espionage, Intelligence, and Security**, v. 1. Farming Hills: Thomson Gale, 2004.

espionagem que forem conduzidas diretamente ou patrocinadas por um Estado, ainda que se reconheça ser comum a prática de espionagem por sociedades empresárias privadas com finalidades econômicas. Por outro lado, a pesquisa inclui em seu âmbito de análise as atividades de inteligência e espionagem que tenham por sujeito passivo indivíduos ou sociedades empresárias.

Não é comum que Organizações Internacionais se empenhem em atividades de espionagem, exatamente em razão do fato de que o envolvimento de vários Estados no processo dificultaria o segredo da operação e exigiria um complicado consenso político sobre uma operação naturalmente clandestina, notadamente em organizações que contam em sua composição com Estados rivais. Não obstante, em organizações formadas por alianças militares, como por exemplo, na Organização do Tratado do Atlântico Norte (OTAN), não seria surpresa encontrar mecanismos de espionagem direcionados a Estados inimigos.⁴⁷

É possível, por outro lado, que os Estados se utilizem de empresas privadas na prestação de serviços terceirizados de inteligência (cf. seção 1.3). Nesse caso, tratando-se de atividades patrocinadas por Estados, incluem-se nos limites materiais da tese.

Como a pesquisa se propõe a uma compreensão sistemática e abrangente sobre a inteligência numa dimensão internacional, não se preocupa em eleger Estados específicos para limitar sua investigação. Todavia, não se pode ignorar o fato de que os Estados Unidos possuem a mais avançada estrutura de inteligência de Estado do mundo, a que corresponde a maior atenção da literatura especializada. Logo, por razões práticas, justifica-se que a inteligência do país, em diversas seções da tese, sirva como parâmetro de análise.

Tal característica poderia servir para denunciar a sujeição da tese a um viés ideológico ocidentalizado. Essa crítica procede, mas sob a certeza de que não se poderia escapar desse tipo de enviesamento. Toda escolha metodológica implica uma escolha ideológica, o que se reflete na definição do referencial teórico, dos autores da bibliografia selecionada e nos próprios limites materiais da pesquisa, que irão estabelecer o campo de estudo. Mesmo os idiomas que o autor de uma tese domina irão refletir uma opção e estabelecer limites de investigação a determinada

⁴⁷ Na Organização do Tratado do Atlântico Norte (OTAN), o “*NATO Intelligence Fusion Centre*” (NIFC) coordena as atividades de inteligência da organização. Cf. <<http://web.ifc.bices.org/index.htm>>.

cultura científica. São escolhas que precisam ser feitas para a construção de uma tese que inevitavelmente revelarão uma posição ideológica do autor.

Por fim, como limite cronológico, se busca principalmente analisar o período compreendido entre 11 de setembro de 2001, quando o surgimento de um novo paradigma de segurança e atividades de inteligência pode ser identificado em razão dos ataques terroristas nos Estados Unidos, até o final do ano de 2016. Isso não impediu, no entanto, que eventos anteriores a esse período fossem mencionados no curso do trabalho com finalidades exemplificativas.

IV Hipóteses sugeridas

A hipótese de uma tese é uma resposta virtual para problemas reais que o pesquisador se compromete a estudar; é a solução precária que ele oferece, que pode vir a se confirmar ou não. Trata-se da faceta mais íntima da relação entre o problema e o pesquisador, verdadeira manifestação de sua criatividade, pelo que possui ele ampla margem de liberdade para formular soluções que acredite serem as mais plausíveis para o desfecho da investigação.

Como discutido na Introdução, o problema inicial a partir do que a tese se desenvolve é a maneira irreflexiva de que os Estados abordam as atividades de espionagem e a insegurança jurídica quanto à licitude dessas atividades segundo o Direito Internacional. A partir disso apresenta-se então uma estrutura hipotética composta por três asserções inter-relacionadas:

- a) A *escassez de parâmetros normativos* de Direito Internacional disponíveis para aferir a licitude da espionagem estatal e a *abordagem irreflexiva* que os Estados sustentam perante a atividade caracteriza um ambiente de *tolerância jurídica e política* da atividade;
- b) A *tolerância das atividades* de espionagem pode ser aferida em *graus*, de acordo com sua modalidade;
- c) As *causas da tolerância da espionagem internacional* são determinadas por *relações de poder*;

- d) O ambiente de *tolerância da espionagem internacional* favorece a conservação do *status quo* de grandes potências da inteligência;
- e) O ambiente de *tolerância da espionagem internacional de segredos de Estado* atenua o nível de incerteza no dilema da segurança.

V Referenciais teóricos e premissas metodológicas

Apesar de não se tratar propriamente de um referencial teórico, um marco central da tese se encontra na divulgação de documentos classificados feita por Edward Snowden em 2013. Não apenas pela relevância do conteúdo dos documentos mas também pelo próprio ato do vazamento, que guarda a conotação de um deliberado inconformismo com as práticas da inteligência dos Estados Unidos e de seus principais aliados. A divulgação da documentação repercutiu de forma impactante pela sociedade civil e governos de outros Estados e agora sabemos mais sobre o caráter e abrangência das práticas de coleta de informação. Como observaram Zygmunt Bauman e outros sobre as revelações de Snowden:

Precisamente o que nós sabemos, o que nós não sabemos, e o que nosso limitado conhecimento acrescenta permanece incerto, de forma a desafiar tanto a análise acadêmica quanto nosso senso de como nós devemos responder através de políticas, procedimentos, instituições e ações coletivas.⁴⁸

Dessa forma, esta tese, como a maioria do que se escreve sobre inteligência de Estado após tais divulgações, é uma tentativa de oferecer uma resposta acadêmica a esse novo paradigma.

Por ser descritiva a análise feita nos seus três primeiros capítulos, não se preocupou em revesti-la de uma estrutura teórica. Apenas se teve o cuidado ali de buscar sólido suporte fático e referências em fontes confiáveis.

⁴⁸ “*Precisely what we know, what we don’t know, and what our limited knowledge adds up to remains uncertain, in ways that challenge both scholarly analysis and our sense of how we should respond through policies, procedures, institutions and collective actions*”. BAUMAN, Zygmunt; BIGO, Didier; ESTEVES, Paulo; GUILD, Elspeth; JABRI, Vivienne; LYON, David; WALKER, R. B. J. After Snowden: Rethinking the Impact of Surveillance. **International Political Sociology**, v. 8, 2014. p. 134.

A tarefa do capítulo 4 é eminentemente dogmática. Algumas situações ali analisadas exigiram uma simples operação de subsunção, enquanto outras demandaram maiores esforços hermenêuticos e argumentativos. Nesses casos, adotou-se uma abordagem crítica, seja quando se detém em reflexões mais profundas sobre argumentos repetidos indiscriminadamente na literatura sobre os problemas que aqui são analisados, seja frente a conceitos estruturantes do Direito Internacional, tais como “soberania” e “não-intervenção”. Isso não significa que a análise seja precisamente balizada por proposições de Estudos Críticos do Direito (*Critical Legal Studies*).⁴⁹ De qualquer forma, irá se notar, é ela crítica em sua tônica, o que é resultado da influência que o pensamento de autores por ele inspirados tiveram sobre esta tese, especialmente o de Martti Koskenniemi.

Já os capítulos 5 e 6 cuidam, respectivamente, da análise das causas e consequências da tolerância da espionagem internacional. Obviamente, essa investigação encerra considerações metajurídicas que não podem, portanto, ser resolvidas nos limites da Teoria do Direito Internacional. Recorre-se então a estudos de Relações Internacionais para compreender o fenômeno.

A Teoria das Relações Internacionais se desdobra em várias vertentes que por sua vez apresentam variantes internamente, criando assim uma multitude de linhas de pensamento e modelos teóricos. Obviamente, cada autor apresentará uma teoria única, com premissas e outras particularidades próprias. Não obstante, traços comuns ou mesmo semelhantes entre uns e outros permitem reuni-los em grupos – ou “escolas” – principalmente para fins de sistematização da disciplina. Dessa forma, pode-se indicar dentre as teorias das Relações Internacionais: o *realismo político* (com suas variantes *realismo clássico*, *realismo estrutural* ou *neorrealismo* e suas divergências internas entre o *realismo ofensivo* e *realismo defensivo*); *liberalismo*; *institucionalismo*; *escola inglesa*; *abordagens críticas*, como marxistas e feministas; *construtivismo*, entre outras vertentes.

⁴⁹ Um trabalho que se pretenda perfeitamente adequado às proposições dos *Critical Legal Studies* deve partir de uma crítica ampla ao modelo liberal e formalista que orienta a argumentação no Direito Internacional. Para uma discussão sobre os resultados da aplicação das proposições dos *Critical Legal Studies* ao Direito Internacional Público conferir: PURVIS, Nigel. *Critical Legal Studies in Public International Law*. **Harvard International Law Journal**, v. 32, n. 1, 1991. Para a crítica ao modelo liberal de Direito Internacional conferir: KOSKENNIEMI, Martti. **From Apology to Utopia: The Structure of International Legal Argument**. Cambridge University Press, 2005. Capítulo 2. Genericamente, conferir: UNGER, Roberto Mangabeira. *The Critical Legal Studies Movement*. **Harvard Law Review**, v. 96, n. 3, 1983.

Como se nota, extrapolaria os objetivos desta tese uma análise em profundidade dessas diversas teorias. Mesmo porque, a escolha de um referencial teórico para orientar uma pesquisa não é uma questão de se definir qual é a “correta” rechaçando-se as “erradas”, mas sim de identificar com propriedade qual possui as premissas mais adequadas para o teste das hipóteses que foram formuladas.

Dessa forma, optou-se por analisar as hipóteses sugeridas segundo as proposições do *realismo político*, que encerram valiosas contribuições à compreensão das relações de poder entre os Estados. Ao alerta que tal assertiva certamente causa no leitor, especialmente no jusinternacionalista, responde-se com uma análise das críticas que são, muitas vezes irrefletidamente, dirigidas ao realismo. Identificou-se uma grande carga de preconceito e caricaturização que são associadas a esta corrente teórica, o que aconselhou uma revisitação aos chamados *realistas clássicos*. Após uma revisão de suas principais proposições, verificou-se a perfeita compatibilidade entre o realismo político e o Direito Internacional, ao contrário do que frequentemente se alega na literatura. (seções 5.1 e 5.2).

Outro esclarecimento metodológico importante diz respeito às tentativas de aproximação entre Direito e Relações Internacionais, que com frequência são encaradas sob suspeitas. Jusinternacionalistas são ávidos em demonstrar uma pretensa “objetividade” do Direito Internacional que lhe garantiria identidade e independência da Política⁵⁰ de forma que a clássica separação entre o estudo do Direito Internacional e o das Relações Internacionais foi convenientemente recepcionada entre nós.

Alguns atribuem a cisão entre os dois domínios à influência do realismo político no pós-segunda guerra mundial⁵¹ e a recente reaproximação entre as

⁵⁰ A objetividade do Direito Internacional face a Política seria decorrência de dois atributos: sua *normatividade*, que se traduz no fato de que o Direito diz o que os Estados devem fazer, não se reduzindo a uma descrição daquilo que eles fazem e sua *concretude*, traduzida na qualidade de ser “menos dependente de crenças subjetivas sobre o que a ordem entre os Estados deva ser”. Koskenniemi mostra como essas duas operações intelectuais não podem ser coerentemente mantidas ao mesmo tempo: “*these requirements tended to overrule each other. A doctrine with much concreteness seemed to lose its normative nature and end up in descriptive apology. A truly normative doctrine created a gap between itself and State practice in a manner which made doubtful the objectivity of the method of verifying its norms. It ended up in undemonstrable utopias*”. KOSKENNIEMI, M. **From Apology**... *op. cit.* p. 58.

⁵¹ “*The dominance of the realist, and later, neorealist school of thought in international relations in the post-World War II era was perhaps the most significant reason for the divide between international law and international relations, as the realist school tended to promote the argument that law was largely derivative of international power politics*”. BIERSTEKER, Thomas J.; SPIRO, Peter J.;

disciplinas é uma conquista reivindicada na literatura *institucionalista e liberalista*.⁵² De forma mais incisiva, Martti Koskenniemi atribui à influência do realismo no pensamento da política norte-americana na segunda metade do século XX um efeito de ceticismo às regras de Direito Internacional, o que conduziu a um pragmatismo político direcionado a estratégias imperialistas.⁵³ Em outra oportunidade denuncia os efeitos prejudiciais que projetos de interdisciplinaridade provocam no Direito Internacional⁵⁴, posição também sustentada por Jan Klabbers.⁵⁵

Note-se, no entanto, que o recurso metodológico adotado nesta tese não é uma simbiose de proposições do Direito Internacional e das Relações Internacionais. Não se sugere interdisciplinaridade no nível epistemológico, conceitual e metodológico desses dois domínios. A aproximação que se sugere aqui é de caráter instrumental. Justifica-se na medida em que se pretende investigar as causas da tolerância da espionagem internacional – o que, como se discutirá ao longo do trabalho, é uma qualidade juridicamente determinada, traduzida na carência de regras – mas que não pode ser explicada estritamente nos limites do Direito. De fato, há diferença entre, de um lado, se utilizar de duas coisas por se acreditar que podem elas contribuir, cada qual a sua maneira, na resolução de um problema, e, de outro, se valer de duas coisas como se uma só fossem.

SRIRAM, Chandra Lekha; RAFFO, Veronica. **International Law and International Relations: Bridging theory and practice**. Routledge, 2007. p. 4.

⁵² Por exemplo: SLAUGHTER, Anne-Marie; TULUMELLO, Andrew S.; WOOD, Stepan. International Law and International Relations Theory: A New Generation of Interdisciplinary Scholarship. **The American Journal of International Law**, v. 92, n. 3, pp. 367-397, 1998; ABBOTT, Kenneth W. Modern International Relations Theory: A Prospectus for International Lawyers. **Yale Journal of International Law**, 1989 e KEOHANE; Robert O. International Relations and International Law: Two Optics. **Harvard International Law Journal**, v. 38, n. 2, 1997.

⁵³ “[...] a pervasive rule-skepticism that turned the attention of academic lawyers from exegetic work with treaties, cases, and formal diplomacy to broader aspects of international co-operation and conflict. The legal profession re-imagined itself as a participant in international policy as advisers and decision-makers in governments, international organizations, and businesses, pursuing a variety of interests and agendas. Public international lawyers increasingly conceived international law from the perspective of a world power, whose leaders have “options” and routinely choose among alternative “strategies” in an ultimately hostile world”. KOSKENNIEMI, Martti. **The Gentle Civilizer of Nations: the rise and fall of international law 1870-1960**. Cambridge University Press, 2004. p. 475.

⁵⁴ *Idem*. Law, Teleology and International Relations: An Essay in Counterdisciplinarity. **International Relations**, v. 26, n. 1, 2011.

⁵⁵ KLABBERS, Jan. The Relative Autonomy of International Law or the Forgotten Politics of Interdisciplinarity. **Journal of International Law & International Relations**, v. 1, 2005. Argumentando contra a ideia de que a aproximação entre Direito e Relações Internacionais é desfavorável àquele, conferir: POLLACK, Mark. A. Is International Relations Corrosive of International Law? A reply to Martti Koskenniemi. **Temple International Law and Comparative Law Journal**, v. 27, n. 2, 2013.

Vale dizer ainda que a escolha do realismo político como referencial teórico para a tese implica uma *opção descritiva* para explicar o fenômeno da tolerância da espionagem internacional, não uma *opção prescritiva* de política externa. Em outros termos, acredita-se que o realismo seja uma boa explicação para alguns fenômenos das relações internacionais, especialmente aqueles relacionados ao exercício do poder, mas isso não significa necessariamente que se recomende a adoção de políticas realistas como opção de política externa. Expressando a mesma distinção, Jack Donnelly afirma:

Normativamente, eu me rebelo contra o mundo descrito na teoria realista e rejeito o realismo como uma teoria prescritiva de política externa. Analiticamente, todavia, eu não sou mais um antirrealista do que sou um realista. Realismo [...] é uma limitada porém poderosa e importante abordagem e um conjunto de conhecimentos sobre as relações internacionais.⁵⁶

Estabelecida esta ressalva, sugere-se que eventos importantes nas últimas décadas, alguns bem recentes, mostram que a cooperação e a proliferação de regimes liberais pelo mundo, que eram aguardadas por autores avessos ao realismo e entusiasmados com o fim da guerra fria, não se afirmaram como se esperava. Assim, favorecem um retorno às teses realistas:

- A política da guerra ao terror dos Estados Unidos que se seguiu aos ataques de 11 de setembro de 2001 levaram o país à guerra e ocupação do Iraque e Afeganistão (seção 2.1) e, sob versões mais moderadas, à intervenção na Líbia (2011) e ao apoio à campanha saudita no Iêmen (2015);
- Os valores liberais que entusiastas apontaram nos movimentos populares de países árabes que ficaram conhecidos como “primavera árabe” de 2011, foram ofuscados pelo soerguimento de outros regimes autoritários – talvez com exceção apenas da Tunísia, que efetivamente estabeleceu uma democracia a partir de então;

⁵⁶ “Normatively, I rebel against the world described in realist theory and I reject realism as a prescriptive theory of foreign policy. Analytically, however, I am no more an anti-realist than I am a realist. Realism, I will argue, is a limited yet powerful and important approach to and set of insights about international relations”. DONNELLY, Jack. Realism. In: BURCHILL, Scott; LINKLATER, Andrew; DEVETAK, Richard; DONNELLY, Jack; PATERSON, Matthew; REUS-SMIT, Christian; TRUE, Jacqui. **Theories of International Relations**, 3 ed., Palgrave Macmillan, 2005. p. 29.

- A política de reafirmação da Rússia como potência mundial. Disso é sintoma o conflito militar com a Geórgia em 2008, a anexação da península da Crimeia em 2014 e as intervenções na Guerra da Síria;
- A expansão militar e econômica da China como sinal de ascensão de uma nova superpotência. Sua campanha de expansão territorial sobre ilhas do Mar do Sul da China é palco de um atrito crescente e preocupante com os Estados Unidos e aliados na região;
- A política de provocação da Coreia do Norte perante o sul, o Japão e os Estados Unidos, evidenciada pelos insistentes testes com mísseis balísticos a que a ONU responde com uma série de sanções econômicas;
- Crescimento do número de ataques terroristas de inspiração radical islâmica;
- A Guerra Civil da Síria, que já perdura desde 2011, já assistiu à intervenção russa, francesa e americana e não sinaliza qualquer possibilidade de solução a curto prazo;
- Crise dos refugiados, que já somam números comparáveis aos da segunda guerra mundial;
- A recente opção da população do Reino Unido por se retirar da União Europeia, que foi fortemente influenciada por uma rejeição à política migratória da União. Ao mesmo tempo o crescimento de movimentos de extrema direita em outros países europeus, especialmente na França, colocam em risco a própria existência da União e as aspirações liberais de seus entusiastas;
- A retirada de Gâmbia, Burundi e África do Sul do Tribunal Penal Internacional, como sintoma de uma crescente insatisfação de países africanos com aquilo que denunciavam ser um viés ocidentalizado da corte.

Obviamente, nenhum desses eventos – arbitrariamente escolhidos, é verdade – evidenciam por si só opções ou resultados de política internacional deliberadamente orientados pela lógica realista. Outros fatos importantes que aconteceram pós-guerra fria sinalizam fortes níveis de cooperação, a exemplo dos sucessos da liberalização do comércio internacional – apesar do atual impasse da Rodada Doha – a atuação global das agências especializadas da ONU e a complexa e profícua integração regional europeia. Todavia, tomados em conjunto, os eventos mencionados ilustram uma conjuntura altamente propensa ao conflito internacional, em que várias das promessas liberais de promoção da cooperação, segurança, democracia e direitos humanos se converteram em dolorosas decepções. Nesse caso, a razão do realismo não é a de se contrapor à agenda liberal, mas sim, e antes de qualquer coisa, alertar para a atual precariedade de suas instituições – inclusive do Direito Internacional – e, por consequência, dos riscos de a elas se confiar a manutenção da paz internacional.

VI Alguns comentários sobre a técnica de redação da tese

O texto da tese foi formatado de acordo com as normas da Associação Brasileira de Normas Técnicas (ABNT) 6023 sobre as referências; 10520 sobre citações e 14724 sobre as regras gerais para elaboração de trabalhos acadêmicos.

Todos os endereços de páginas de *internet* citados nas referências foram reaceessados ao final do trabalho e estão ativos na forma de *hiperlink* na versão digital do texto.

Citações em língua estrangeira foram traduzidas para o português no corpo do texto, acompanhadas do respectivo original em nota de rodapé. Já as citações em língua estrangeira que são transcritas apenas em nota de rodapé e as epígrafes que procedem aos títulos de capítulos não foram traduzidas.

A tradução de siglas foi apenas realizada quando a versão em português for comumente mais utilizada no Brasil. Assim, preferiu-se por utilizar no corpo do texto, por exemplo, a sigla OTAN ao invés de *NATO*, mas, por outro lado, *CIA* e *FBI* ao invés de *ACI* e *EFI* que seriam formas em português não reconhecíveis de imediato.

Os trechos de publicações anteriores de minha autoria que são repetidos ou adaptados no texto da tese são assim discriminados em nota de rodapé.

VII Algumas notas sobre códigos utilizados em documentos classificados

No curso do trabalho e nos anexos serão apresentados muitos documentos originalmente classificados que contém códigos destinados a especificar o nível de classificação do documento, o tipo de inteligência a que ele se refere e quais Estados estão autorizados a receber a informação ali contida. Um exemplo seria a seguinte codificação: **TS//SI//NF** que designa um documento *Top Secret*; qualificado como *Special Intelligence*; vedado a estrangeiros, ou seja *No Foreign*.

Ainda que a compreensão desses códigos não seja imprescindível para a leitura dos documentos, para possibilitar um entendimento mais apurado apresenta-se uma breve explicação do significado de alguns deles abaixo. Optou-se por trazer esta listagem aqui e não na lista de siglas e abreviaturas para permitir uma explicação mais detalhada do que sua mera decodificação.

U – “*Unclassified*”; Documento ou trecho do documento não classificado.

C – “*Confidential*”; Documento ou trecho do documento de nível de classificação “Confidencial”.

S – “*Secret*”; Documento ou trecho do documento de nível de classificação “secreto”.

TS – “*Top Secret*”; Documento ou trecho do documento de nível de classificação “altamente secreto”.

FOUO – “*For Official Use Only*”; Documento ou trecho do documento restrito ao uso oficial.

SI – “*Special Intelligence*”; informação relativa à interceptação de comunicações, até 2011 codificado como COMINT, “*Communications Intelligence*”.

OC / ORCON – “*Originator Controlled*”; O órgão de onde se origina o documento controla sua disseminação e/ou publicação.

NF / NOFORN – De conhecimento vedado a estrangeiros, isto é, “*No Foreign*”.

FVEY – Documento a ser compartilhado com a rede de inteligência composta por Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia, os chamados “*Five Eyes*”.

REL TO – Documento ou trecho de documento autorizado para compartilhamento, seguido do código dos Estados e/ou órgãos que terão acesso ao documento. Exemplo: “REL TO FVEY” designa um documento a ser compartilhado com os membros da rede *Five Eyes*.

1 A ATIVIDADE DE INTELIGÊNCIA ESTATAL

*"Intelligence work is in essence nothing more than the search for the single best answer".*⁵⁷
(Sherman Kent)

1.1 O que é e para que serve a inteligência de Estado

Agências de inteligência podem coletar informação para propósitos de segurança nacional, condução da diplomacia e da política externa, elaboração da política econômica, conflitos militares, operações humanitárias, entre um amplo espectro de outras atividades estatais. Seja qual for a finalidade da obtenção da informação, em essência, inteligência é uma ferramenta de conhecimento. Realiza-se inteligência para reunir informação com mais eficiência, o que significa obter informação relevante, de melhor qualidade e em maior número do que se poderia conseguir sem um aparato organizado de coleta.

Não obstante, a mera coleta da informação "bruta", ainda que feita de forma organizada e sistemática, normalmente não será suficiente para a exata compreensão de suas implicações. Isso exigirá submetê-la a um rigoroso procedimento de análise, que poderá envolver decifração de informações criptografadas, estudos técnico-científicos como o exame de imagens de satélites, por exemplo, entre outras tantas espécies de verificação.

O produto dessa análise é utilizado para informar líderes e outras autoridades de Estado – os chamados "consumidores" – para que assim possam aprimorar seu processo decisório em questões estratégicas de Estado, como por exemplo conflitos militares, segurança interna, defesa do território, diplomacia e política externa. No desempenho dessas variadas funções, autoridades estatais serão supridas de dados e pareceres confiáveis para a tomada de decisão, através da informação qualificada pela inteligência.

Inteligência, portanto, não é um fim em si mesmo. O produto da inteligência é a informação e seu objetivo a decisão. Quanto mais confiáveis e precisas forem a informação e a análise de suas implicações, maiores as chances de se obter o

⁵⁷ KENT, Sherman. **Strategic Intelligence for American World Policy**. Princeton University Press, 1949.

resultado esperado através de determinada decisão. De certa forma, é possível afirmar que o recurso à inteligência de Estado é uma manifestação de aderência a procedimentos racionais de governabilidade.⁵⁸

Portanto, pode-se definir a **inteligência de Estado como sendo a atividade estatal através da qual são coletadas e analisadas informações de forma organizada e sistemática com a finalidade de orientar o processo decisório de suas autoridades**. Trata-se de conceito próximo do que Lock K. Johnson denomina de “inteligência estratégica”, isto é, “os esforços de líderes para entender os riscos e ganhos potenciais a nível nacional e internacional”.⁵⁹

Uma definição também semelhante foi proposta por Myres McDougal, Harold Lasswell e Michael Reisman:

A função da inteligência engloba a coleta, avaliação e disseminação de informação relevante para o processo decisório e pode incluir previsão baseada em tal informação, assim como planejamento para futuras contingências.^{60 61}

Na seção seguinte será descrito o funcionamento de um serviço de inteligência, através da análise de seus principais vetores de atuação: a requisição, a coleta, o processamento, a análise e a disseminação de informações.

1.2 Como os Estados realizam inteligência?

Dizer que a inteligência estatal é realizada de forma organizada e sistemática significa dizer que é ela operada por órgãos do governo (agências) e de forma profissional. Ainda que dotadas de estruturas diferentes, em essência o que todas as agências de inteligência fazem consiste em coletar, analisar e disseminar informações para líderes de Estado e outras de suas autoridades.

⁵⁸ Segundo Michael Herman: “*Gathering and using intelligence is also part of what is now expected of modern government's adherence to rational procedures in other matters*”. HERMAN, Michael. **Intelligence Power in Peace and War**. Cambridge University Press, 1999. p. 139.

⁵⁹ “[...] *strategic intelligence, that is, the attempts by leaders to understand potential risks and gains on a national or international level*”. JOHNSON, Lock K. (org.) **Handbook of Intelligence Studies**, London: Routledge, 2007. p. 1.

⁶⁰ “*The intelligence function comprises the gathering, evaluation and dissemination of information relevant to decision-making, and may include prediction based on such information, as well as planning for future contingencies*.” MCDUGAL, Myres S.; LASSWELL, Harold D.; REISMAN, W. Michael. *The Intelligence Function and World Public Order*. **Temple Law Quarterly**, v. 46, n.3, 1973. p. 365.

⁶¹ No mesmo sentido, CHEN, Lung-Chu. **An Introduction to Contemporary International Law: a policy-oriented perspective**. Oxford University Press, 3 ed., 2015. p. 403.

É comum encontrar na literatura a associação dessas atividades em uma lógica cíclica – o chamado “ciclo da inteligência”.

A ideia é a de que o ciclo se iniciaria com a requisição de autoridades por informações a respeito de determinado tópico, o que provocaria a coleta da informação. Uma vez obtida, a informação seria analisada e posteriormente encaminhada para as autoridades estatais, permitindo assim que se iniciasse outro ciclo com nova requisição.

Essa noção pode ser aceita desde que se tenha em mente que se trata de uma simplificação. Existem diversas complexidades que, dentro e fora dessas etapas, desafiam a ideia de inteligência como um ciclo. Nas seções seguintes busca-se explorar com mais detalhes as etapas do processo, não apenas para desconstruir o mito do ciclo da inteligência, mas para apresentar uma descrição mais real da atividade.

1.2.1 O processo de requisição de autoridades por informações

O processo da inteligência estatal se inicia, na realidade, com a percepção de autoridades públicas da necessidade de saber, quando confrontados com a tarefa de decidir. Como discutido anteriormente, o conhecimento de informações precisas a respeito de determinado assunto facilita o processo decisório e, assim, autoridades de alto-escalão irão conferir o norte dos serviços de inteligência de acordo com suas necessidades por saber.

Nos Estados Unidos, o acerto das prioridades da comunidade de inteligência é feito através do mecanismo “*National Intelligence Priorities Framework*” (NIPF), coordenado no âmbito do Escritório do Diretor de Inteligência Nacional (*Office of the Director of National Intelligence – ODNI*)⁶² (v. seção 1.3, i). O procedimento inclui entrevistas com os “consumidores” para compreender suas reais necessidades por informação. Estes podem ser o Presidente e o Vice-Presidente, o

⁶² OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. **Intelligence community directive 204:** National Intelligence Priorities Framework. Disponível em: <<http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf>>

Secretário de Estado e o Secretário de Defesa, o Procurador-Geral, chefes das forças armadas, entre outras autoridades e agências.⁶³

O processo de requisição visa, portanto, orientar o trabalho da inteligência, o que em essência é uma questão econômica: sendo limitado seu orçamento e as capacidades de coleta, é importante concentrar esforços na busca pelas informações mais sensíveis ao interesse nacional. Mas ainda que as autoridades possam externar suas preocupações e solicitar informações em determinado sentido, a inteligência sustenta a iniciativa para coletar informações que possam antecipar o surgimento de uma necessidade.⁶⁴ Nos termos colocados por J. Ransom Clark:

Coletores de todos os tipos – sejam humanos ou técnicos – repentinamente podem ser confrontados com oportunidades de adquirir informação que poderia ser útil mas não aparece em nenhuma lista. Eles raramente irão optar por deixar passar tal chance. Similarmente, é esperado que analistas sejam especialistas em seu campo de atuação, e eles devem estar preparados para propor e explorar questões que não foram formalizadas pelo processo de requisição.⁶⁵

Além disso, sistemas sofisticados de inteligência possuem bases de dados tão grandes (cf. seção 1.2.5, “Inteligência Básica”) que a tarefa das agências normalmente consiste no preenchimento de “hiatos de informação”, concentrando esforços na busca por informações sobre o que ainda se ignora. Segundo Arthur S. Hulnick, a necessidade de preenchimento dessas lacunas, acima das requisições políticas, é o que verdadeiramente impulsiona os serviços de inteligência.⁶⁶

⁶³ OLESON, Peter C. **Who Are the Customers for Intelligence?** [draft paper] Disponível em: <[http://www.afio.com/publications/OLESON_Who%20are%20customers%20of%20intel%20\(rev\)_Draft_2014Feb10.pdf](http://www.afio.com/publications/OLESON_Who%20are%20customers%20of%20intel%20(rev)_Draft_2014Feb10.pdf)>

⁶⁴ Um interessante exemplo dessa tentativa de antecipação é um estudo do escritório de pesquisas da CIA, datado de 1974, em que se tentava “prever” as então denominadas *Key Intelligence Questions (KIQs)* para a década de 80. O documento antes secreto, hoje desclassificado, pode ser lido em: CENTRAL INTELLIGENCE AGENCY. **Some Likely Intelligence Questions for the 1980’s**. Disponível em: <http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0001246423.pdf>

⁶⁵ “Collectors of all types — whether human or technical — suddenly can be confronted with opportunities to acquire information that may be meaningful but appears on no list. They will rarely elect to pass up such chance moments. Similarly, analysts are expected to be the experts in their fields, and they must be prepared to ask and explore questions that have not been formalized by the requirements process”. CLARK, Ransom J. **Intelligence and National Security: A Reference Handbook**. London: Praeger Security International, 2007. p. 26-27.

⁶⁶ HULNICK, Arthur S. What’s wrong with the Intelligence Cycle? In JOHNSON, Lock K. (org.) **Strategic Intelligence**, v. 2, Praeger Security International, 2007. p. 2-3.

Por outro lado, algumas questões são de notório interesse para um Estado, de forma que qualquer informação a elas pertinente será alvo da inteligência. Proliferação nuclear e conflitos no oriente médio, por exemplo, são temas que permanentemente interessam aos Estados Unidos. Logo, o sistema de coleta estará sempre atento a informações de tal natureza, sem que precise ser orientado a tanto.

1.2.2 A atividade de coleta de informações

Atualmente, os sistemas de inteligência mais sofisticados podem contar com grande variedade de mecanismos de coleta de informação, empregados tanto nas vias ordinárias da inteligência quanto na espionagem. São as chamadas “disciplinas de coleta”, a saber:⁶⁷

a) Inteligência de fontes humanas (*Human-Source Intelligence – HUMINT*)

A modalidade mais antiga de coleta de informações, a inteligência de fontes humanas é tradicionalmente conduzida por agentes infiltrados em território estrangeiro ou oficialmente acreditados junto ao corpo diplomático, ou mesmo pessoas lá recrutadas clandestinamente. Enquanto diplomatas possuem fontes confidenciais compatíveis com o *status* e a prática da diplomacia – normalmente autoridades oficiais – as pessoas com as quais ele não pode se encontrar sem que haja risco para as relações diplomáticas serão alvo dos chamados “*case officers*”, a serviço de agências de inteligência.⁶⁸

Provavelmente a manifestação histórica mais remota do Direito Internacional, com sólida evolução costumeira, a atividade diplomática⁶⁹ possui peculiaridades que favorecem significativamente a obtenção da informação em território estrangeiro. Embora a Convenção de Viena sobre Relações Diplomáticas de 1961 não se refira

⁶⁷ DEPARTMENT OF DEFENSE. **Dictionary of Military and Associated Terms**. 2015. Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>; DATA Gathering. **Intelligence.gov**, Disponível em: <<http://www.intelligence.gov/mission/data-gathering.html>>

⁶⁸ HERMAN, M. *op. cit.* p. 61. Sobre a organização do serviço clandestino da CIA, conferir seção 1.3, item ii.

⁶⁹ Segundo Malcolm Shaw, “*Rules regulating the various aspects of diplomatic relations constitute one of the earliest expressions of international law. Whenever in history there has been a group of independent states co-existing, special customs have developed on how the ambassadors and other special representatives of other states were to be treated*”. SHAW, Malcolm N. **International Law**. Cambridge: Cambridge University Press, 6 ed., 2008. p. 750-751.

expressamente ao exercício da inteligência por diplomatas, ressaltam Myres McDougal *et al.* que ele é geralmente aceito como “finalidade correlativa” da atividade diplomática e largamente tolerado pelos Estados, especialmente sob inspiração de reciprocidade.⁷⁰

De fato, incluem-se entre as funções da missão diplomática a de “inteirar-se por todos os meios lícitos das condições existentes e da evolução dos acontecimentos no Estado acreditado e informar a esse respeito o Governo do Estado acreditante”, como se lê no art. 3 da Convenção. Além disso, favorece o exercício da inteligência as garantias de livre comunicação da missão com seu governo e de inviolabilidade dos arquivos, documentos, correspondências e da mala diplomática da missão (art. 24 e 27). É preciso considerar ainda que o agente diplomático goza de imunidade de jurisdição penal no Estado acreditado, o que poderia lhe encorajar a se imiscuir em atividades de espionagem. Obviamente, caso o diplomata seja flagrado em tal espécie de atividade, obtendo informações classificadas do Estado acreditado, poderá ser declarado *persona non grata* (art. 9) e dele ser expulso por ter excedido em suas atribuições e engajado em práticas incompatíveis com a diplomacia.⁷¹

Paralelamente, o Estado poderá se valer de agentes de inteligência que podem ingressar em território estrangeiro junto ao corpo diplomático – gozando das mesmas imunidades – ou por outros meios, seja através das vias ordinárias com um passaporte estrangeiro ou mesmo clandestinamente – os chamados *Non-Official-Cover Operatives* (NOCs). A atividade desses agentes pode compreender o recrutamento de informantes e desertores ou mesmo a infiltração em empresas ou em estratos do governo estrangeiro. Existem alguns exemplos emblemáticos dessa figura – o arquétipo do espião:

Richard Sorge – Lendário espião alemão, com forte inclinação comunista, a serviço do *Glavnoye Razvedyvatel'noye Upravleniye* (GRU) – a inteligência militar russa – foi designado para montar a maior rede de espionagem soviética no extremo oriente. Operando sob o disfarce de jornalista, estabeleceu-se inicialmente na China e posteriormente no Japão, a partir de 1933, lá permanecendo durante a Segunda Guerra Mundial. Com o objetivo de suprir a inteligência soviética com informações

⁷⁰ MCDOUGAL, M. *et al. op. cit.* p. 380-381.

⁷¹ CHESTERMAN, S. *op. cit.* p. 1089.

políticas e militares do eixo, Sorge foi capaz de antecipar com precisão a ocorrência da Operação Barbarossa, codinome para a invasão nazista à União Soviética.

Graças a importantes contatos na embaixada alemã em Tóquio, em maio de 1941 Sorge alertava que “Hitler está totalmente determinado a iniciar uma guerra e destruir a União Soviética a fim de adquirir a porção europeia da União Soviética como uma base de grãos e matéria-prima”⁷². Sorge foi inclusive capaz de determinar com grande precisão que o início da invasão se daria entre 20 e 22 de junho de 1941⁷³ – de fato, ela ocorreu em 22 de junho – alertas cuja gravidade foi arrogantemente desprezada por Stálin.⁷⁴

Robert Philip Hanssen – norte-americano, agente do *Federal Bureau of Investigation* (FBI) se voluntariou para espionar em favor da inteligência soviética/russa, obtendo e repassando clandestinamente informações classificadas entre 1976 e 2001, ano em que foi preso. Hanssen repassou ao *GRU* e à *Komitet gosudarstvennoy bezopasnosti* (KGB) – “Comitê para a segurança do Estado”, o principal serviço soviético de inteligência – milhares de páginas de documentos de alta classificação e dezenas de discos de computadores detalhando o planejamento dos Estados Unidos para eventual superveniência de uma guerra nuclear, bem como informações sobre o programa de contrainteligência do país.⁷⁵ Considerado o espião mais danoso da história dos Estados Unidos, atualmente cumpre 15 condenações de prisão perpétua em presídio de segurança máxima, correspondentes a 15 acusações confessas por espionagem.

Oleg Penkovsky (1919-1963) – Coronel russo a serviço do *GRU*, repassou à inteligência americana e britânica informações detalhadas sobre as capacidades militares da União Soviética, informações políticas e identidade de agentes do *GRU* operando em países ocidentais.⁷⁶ Dessas informações, destacavam-se dados sobre bases de lançamentos de mísseis na União Soviética, que em 1962 serviram para

⁷² “Hitler is fully determined to make war upon and destroy the USSR in order to acquire the European area of the USSR as a raw materials and grain base [...]. Cf. RICHELSON, Jeffrey T. **A Century of Spies: Intelligence in the Twentieth Century**. Oxford: Oxford University Press. p. 113.

⁷³ GILBERT, Martin. **A Segunda Guerra Mundial**. Tradução: Ana Luísa Faria; Miguel Serras Pereira. Rio de Janeiro: Casa da Palavra, 2014 [Edição Original de 1989]. p. 213.

⁷⁴ Conta-se que Stálin se referiu a Richard Sorge como “a shit who has set himself up with some small factories and brothels in Japan”. Cf. RICHELSON, J. T. **A Century of Spies... op. cit.** p. 115.

⁷⁵ UNITED STATES DEPARTMENT OF JUSTICE. **A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen**, ago. 2013. Disponível em: <<https://oig.justice.gov/special/0308/final.pdf>> Este documento trata-se de uma versão resumida e não classificada de um relatório altamente secreto de 674 páginas que detalha toda a investigação que precedeu a identificação e prisão do espião.

⁷⁶ HASTEDT, Glenn. **Espionage: a reference handbook**. Santa Barbara: ABC-Clio, 2003. p. 95.

confirmar a existência de instalações semelhantes em Cuba, detectadas por imagens aéreas obtidas em sobrevoos de aviões U-2 na ilha. Em outubro do mesmo ano o Coronel foi “desmascarado” pela *KGB*, sendo posteriormente executado na União Soviética por traição.⁷⁷

Fora esses exemplos mais dramáticos, a inteligência de fontes humanas compreende entrevistas e interrogatórios com dissidentes políticos, asilados, refugiados e migrantes, sendo eles fontes “conscientes” ou não. Nessa última hipótese, a pessoa pode acreditar estar repassando informações para fins jornalísticos ou para uso comercial, por exemplo.⁷⁸ O Canadá, que não conduz inteligência externa com espões, ilustra bem tal abordagem por possuir uma organização relativamente aberta para entrevistar imigrantes e viajantes que possam fornecer informações úteis.⁷⁹

É preciso destacar, por fim, a necessidade de preservação da identidade da fonte humana – seja ela um informante ou um entrevistado – cujo nome normalmente será substituído por um codinome nos relatórios. Nos Estados Unidos, a divulgação de informação classificada que revele ou possa revelar a identidade de agentes secretos de inteligência, informantes e fontes constitui crime federal (50 U.S.C. § 421).⁸⁰

b) Inteligência de Sinais (*Signals Intelligence – SIGINT*)

Em 1938 o General alemão Werner Von Fritsch declarou que a nação com os melhores intérpretes de imagens venceria a próxima guerra. Sua previsão se provou

⁷⁷ A versão mais aceita é a de que *Oleg Penkovsky* tratava-se, de fato, de um desertor soviético colaborando legitimamente com a inteligência britânica e americana, e que sua execução, por sinalizar aos americanos que as informações passadas pelo espião eram de fato verdadeiras, refletiu uma decisão política do *Politburo* de mover a crise dos mísseis para patamares mais seguros. Cf. HASTEDT, G. *op. cit.* p. 96-97. Todavia, uma versão alternativa, sustentada pelo britânico Peter Wright, ex-*Military intelligence 5 (MI5)*, argumenta que *Penkovsky* – cuja execução, afirma ele, teria sido uma farsa – era, na verdade, um espião leal à União Soviética designado para convencer os Estados Unidos de que a capacidade balística intercontinental soviética era menos desenvolvida do que de fato era. Cf. WRIGHT, Peter. **Spy Catcher**. Australia: William Heinemann Publishers, 1987.

⁷⁸ HERMAN, M. *op. cit.* p. 62.

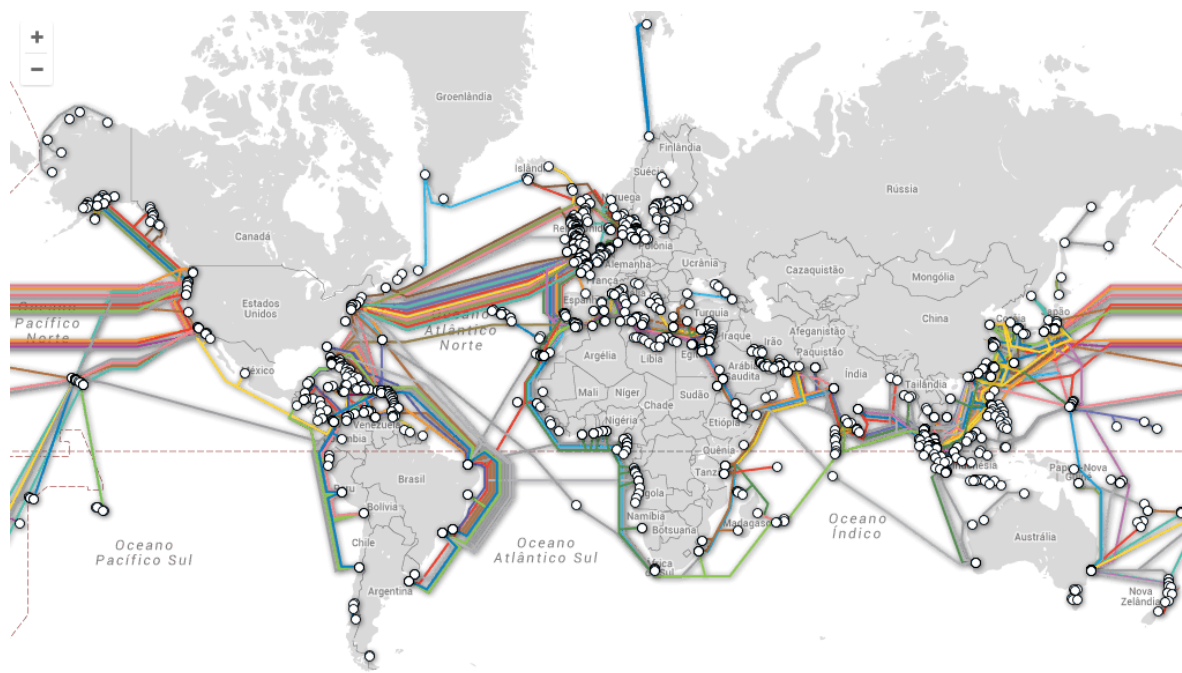
⁷⁹ *Ibidem*. p. 66.

⁸⁰ ELSEA, Jennifer K. Intelligence Identities Protection Act. **Congressional Research Service**, 10 abril 2013.

errônea. Na verdade, os países que detinham a melhor inteligência de sinais foram os vencedores da segunda guerra mundial.⁸¹

Nessa modalidade, a coleta de informações é feita através da interceptação de sinais eletrônicos, seja na comunicação entre pessoas (*Communications Intelligence* – COMINT), entre máquinas (*Electronic Intelligence* – ELINT), ou uma combinação de ambos.

Além de poder consistir na monitoração de comunicações telefônicas, *e-mails*, videoconferências e mensagens de texto de indivíduos, a SIGINT também engloba a interceptação de sinais de rádio, de satélites, de sonares entre outros dispositivos eletrônicos. Pode ser conduzida através de escutas telefônicas, “grampos” em cabos submarinos de fibra ótica, “satélites-espiões”, bases de recepção de sinais instaladas em solo ou em navios e aeronaves entre outros métodos. Outra forma muito comum de interceptação de sinais ocorre através da instalação de antenas e outros tipos de receptores nos telhados de embaixadas e consulados, visando a coleta de informações do Estado acreditado.⁸²



(Mapeamento de cabos submarinos, atualizado até 24 de março de 2016. A versão interativa do mapa pode ser acessada em <<http://www.submarinecablemap.com/>>)

Duas agências se destacam na condução de inteligência de sinais: A NSA, que é a agência responsável pela inteligência de sinais norte-americana e o *United*

⁸¹ Como observado em LATHROP, Charles E. **The Literary Spy**. Yale University Press, 2004. p. 296.

⁸² RICHELSON, J. T. The technical collection of intelligence. In: JOHNSON, L. K. (org.) **Handbook...** *op. cit.* p. 105.

Kingdom Government Communications Headquarters (GCHQ). Uma parceria que se iniciou após a Segunda Guerra Mundial, em 1946, como resultado da cooperação entre os Estados Unidos e o Reino Unido em atividades de inteligência durante o conflito. O consórcio, formalizado no chamado acordo UKUSA⁸³ – então um tratado secreto – posteriormente contou com a adesão do Canadá, da Austrália e da Nova Zelândia, formando a rede de compartilhamento de inteligência conhecida como *Five Eyes* (codinome: *FVEY*).

Um dos mais abrangentes programas operados pela rede é o ECHELON. Trata-se de um sistema de proporções globais de interceptação de comunicações via satélite, ondas de rádio e cabos de fibra ótica – o que teoricamente inclui toda comunicação de telefonia celular e de *internet*. O programa foi objeto de investigações do Parlamento Europeu nos anos de 2000 e 2001, sob preocupações de que a rede *Five Eyes* conduzisse espionagem de informações privadas de cidadãos e empresas europeias o que se confirmou⁸⁴ (cf. seção 4.3.1).

Outro programa que se destaca pela sua intrusividade é o PRISM, codinome para um sistema de vigilância eletrônica global com custo de operação anual de US\$ 20.000.000,00 (vinte milhões de dólares). O sistema é capaz de coletar informações (incluem-se *e-mails*, mensagens de texto e de voz, vídeos, dados armazenados etc.) de grandes companhias de tecnologia e seus principais serviços (*Microsoft, Yahoo, Google, Facebook, Youtube, Skype, AOL, Apple e Verizon*)⁸⁵, por acesso que é obtido através de mandado judicial ou clandestinamente.

A imagem a seguir trata-se de um documento altamente secreto (*Top Secret*), “vazado” entre as revelações de Edward Snowden para a imprensa, ilustrando o sistema de SIGINT global cooperado pelos Estados da rede *Five Eyes*.

⁸³ NATIONAL SECURITY AGENCY. **UKUSA Agreement Release 1940-1956**. Disponível em: <https://www.nsa.gov/public_info/declass/ukusa.shtml>

⁸⁴ “That a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt. [...] What is important is that its purpose is to intercept private and commercial communications, and not military communications”. EUROPEAN PARLIAMENT. **Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)**, 2001. p. 133.

⁸⁵ GREENWALD, Glenn; MACKASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**. 7 jul. 2013. Disponível em: <<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>>



(Fonte: ARCHIVE.ORG. **NSA Worldwide SIGINT/ Defense Cryptologic Platform.**

Disponível em: <<https://archive.org/details/NSA-Defense-Cryptologic-Platform>>)

Os pontos em azul indicam acessos em cabos de fibra ótica de transmissão de dados em alta velocidade, permitindo a coleta massiva de informações na *internet*. Certamente é o maior ativo da rede. Os pontos vermelhos indicam bases regionais instaladas clandestinamente em embaixadas e consulados por todo o mundo. As cidades que abrigam esse tipo de instalação estão listadas na parte superior do documento, onde, vale observar, se inclui Brasília.⁸⁶ Já os pontos em laranja indicam estações de interceptação de comunicações de satélites estrangeiros (daí o codinome FORNSAT - “foreign satellites”). Os pontos amarelos designam a estratégia de “Exploração de Redes de Computadores” (*Computer*

⁸⁶ Segundo informações do blog *electrospaces.net*, especializado em SIGINT, o documento original foi “vazado” sem as censuras na lista de cidades, tendo sido as rasuras apostas por Glenn Greenwald a pedido de Edward Snowden. Cf. NSA’S Global Interception Network. **Electrospaces.net**, 03 dez. 2013. Disponível em: <<http://electrospaces.blogspot.com.br/2013/12/nsas-global-interception-network.html>>

Network Exploitation – CNE). Como destaca a legenda, é composta de mais de 50.000 “implantes”, espécie de vírus que permite acesso a computadores.⁸⁷

c) Inteligência de Imagens (*Imagery Intelligence – IMINT*):

Evoluindo da obtenção de fotografias em sobrevoos de balões a imagens em alta definição por meio de satélites orbitais e *drones*, passando por aeronaves de reconhecimento, a IMINT provê os olhos da inteligência. Além de poder ser realizada através do recurso ótico de câmeras, a IMINT também se vale da radiação infravermelha ou da emissão e reflexão de ondas ultrassônicas em situações em que o objeto não pode ser naturalmente visualizado (ex: visão obstruída por nuvens, ausência de iluminação, locais subterrâneos).⁸⁸

Segundo Jeffrey Richelson, em 2007 o sistema de imagens de satélites operado pelos Estados Unidos era composto por seis satélites que forneciam imagens em tempo real, todos com capacidade para produzir registros por luz visível ou infravermelha e dentre os quais se inclui ao menos um satélite furtivo (*stealth*), capaz de evitar ou dificultar sua detecção por outros Estados.⁸⁹

Além dos Estados Unidos, Reino Unido, Rússia, China, França, Itália, Alemanha, Turquia, Israel, Índia, Coreia do Sul e Japão possuem satélites de reconhecimento por imagens.⁹⁰

⁸⁷ Um exame detalhado sobre o documento, incluindo a razão de não serem destacados no mapa os pontos verdes listados na legenda, pode ser lido em ELECTROSPACES.NET. *op. cit.*

⁸⁸ RICHELSON, J. T. The technical collection... *op. cit.* p. 106.

⁸⁹ *Ibidem.* p. 107.

⁹⁰ Cf. *Ibidem.* p. 107; FEDERATION OF AMERICAN SCIENTISTS. **IMINT Gallery**. Disponível em: <<http://fas.org/irp/imint/>>



(Imagem de satélite de um complexo de edifícios em Abbottabad, Paquistão. Em destaque o local em que Usama Bin Ladin foi morto pelas forças especiais da marinha norte-americana *Seal Team 6*, na operação "*Neptune Spear*", em 02 de maio de 2011. Crédito da Imagem: Digital Globe).

d) Inteligência de fontes abertas (*Open-Source Intelligence* – OSINT)

A inteligência de fontes abertas objetiva a coleta de informações publicamente disponíveis. Trata-se de conceito próximo ao que nesta tese se denomina de inteligência ordinária (v. Metodologia, II, "Parâmetros Conceituais"), com a diferença de que esta última se refere à publicidade não somente da fonte da informação mas também dos mecanismos de coleta.

Ainda que, de fato, a OSINT não objetive a coleta de informações sigilosas, com o surgimento da *internet* e, posteriormente, das redes sociais, tal modalidade ganhou novo e expressivo papel nos atuais aparatos de inteligência estatal. Como reconhecido no “Manual de Fontes Abertas da OTAN”, “excluir o fluxo de informações transmitido pela *internet* seria excluir a maior fonte emergente de dados disponível”.⁹¹

O valor da OSINT é reconhecido na sua capacidade de estabelecer um contexto para a análise de informações providas de outras fontes e modalidades de inteligência. Ao fornecer informações políticas, históricas, sociais e econômicas que estão publicamente disponíveis, a OSINT assume um papel complementar, sobre o que poderão se desdobrar com maior eficiência os métodos de espionagem por HUMINT, SIGINT e IMINT – processo conhecido como inteligência de todas as fontes (*all-source intelligence*).⁹² Com efeito, estima-se que de 80% a 90%⁹³ das informações coletadas por serviços de inteligência provenham de fontes abertas.

Um argumento sofisticado em favor da potencialização da OSINT e, além, de uma estrutura de sociedade e governos abertos, tem por autor Robert David Steele, ex-oficial da CIA, e foi apresentado na obra “*The Open-Source Everything Manifesto: Transparency, Truth and Trust*”. Trata-se de uma proposta ampla de reforma do modelo político e econômico vigente nas sociedades contemporâneas, com fundamento no livre compartilhamento de informações, o que se estende para serviços de inteligência. De acordo com Steele, o serviço de inteligência dos Estados Unidos não é capaz de estudar nada holisticamente, substitui “informação” por “ideologia”, gasta com ineficiência e portanto não é apto a notar as verdadeiras opções e respectivos custos que precisam ser percebidos para o bom processo decisório.⁹⁴ Partindo dessa crítica, o autor sugere um modelo de inteligência difusa e transparente, em que cada cidadão seja educado para ser capaz de coletar, analisar e criticar informações obtidas de fontes abertas, formando assim uma comunidade

⁹¹ “To exclude the information flow carried by the Internet is to exclude the greatest emerging data source available”. NORTH ATLANTIC TREATY ORGANIZATION. **NATO Open Source Intelligence Handbook**, 2001. p. v.

⁹² *Ibidem*. p. 36.

⁹³ A primeira estimativa formulada pelo historiador Sherman Kent e a segunda pelo tenente general Samuel Wilson, como citado no relatório BEST JR., Richard A.; CUMMING, Alfred. Open Source Intelligence (OSINT): Issues for Congress. **Congressional Research Service**, 05 dez. 2015. p. 4.

⁹⁴ STEELE, Robert David. **The Open-Source Everything Manifesto: Transparency, Truth and Trust**. Berkeley: Evolver Editions, 2012. p. xvii

de inteligência interconectada e coesa, com a finalidade última de exercer plenamente as aspirações da democracia direta.⁹⁵

e) Inteligência de Mensuração e Assinaturas (*Measure and Signature Intelligence* – MASINT)

Basicamente é um tipo de inteligência realizada através de sensores. Visa a produção de informações por análise quantitativa e qualitativa dos atributos físicos de alvos e eventos para caracterizá-los, localizá-los e identificá-los, além de informações derivadas de medições técnicas de mensuração do fenômeno físico intrínseco a um objeto ou evento. Envolve um largo espectro de ferramentas tais como ótica, radiofrequência, radiação eletromagnética, acústica, nuclear, sísmica, química dentre outras.

Apesar de ser classificada oficialmente como uma disciplina de coleta, a MASINT, como uma atividade de medição, possui alguns aspectos que seriam melhor descritos como ferramentas de processamento e análise.

f) Inteligência Geoespacial (*Geospatial Intelligence* – GEOINT)⁹⁶

A inteligência geoespacial tem por finalidade reunir informação sobre a atividade humana na superfície terrestre. Trata-se de uma disciplina intimamente associada a conceitos geográficos e sociais, portanto. Realiza-se principalmente através da coleta de imagens, seja ela feita por satélites de reconhecimento⁹⁷, sobrevoos com aeronaves e mesmo câmeras e sensores posicionados no solo. As imagens são combinadas com outras informações geográficas, como por exemplo mapas e dados de posicionamento global.

Em situações em que não é possível a obtenção de imagens diretas (ex: atmosfera nublada obstruindo a visão do satélite ou pessoas e objetos no subsolo),

⁹⁵ *Ibidem.* p. xviii.

⁹⁶ Em fevereiro e março de 2016 tive a oportunidade de participar do curso à distância, obtendo a respectiva certificação, “*Geospatial Intelligence and Geospatial Revolution*”, pela *Pennsylvania State University*.

⁹⁷ Informações sobre cada um dos mais de 1.300 satélites ativos na órbita terrestre podem ser encontradas em gráfico interativo em: YANOFSKY, David; FERNHOLZ, Tim. The World above Us: This is every active satellite orbiting earth. **Quartz**. Disponível em: <<http://qz.com/296941/interactive-graphic-every-active-satellite-orbiting-earth/>>

a inteligência geoespacial é capaz de fornecer dados através de análise do espectro eletromagnético (radiação ultravioleta e infravermelha).

1.2.3 O processamento e a avaliação da informação

A informação “bruta” obtida através das operações de coleta precisa ser “refinada” antes que seja direcionada à análise, o que será feito através do processamento técnico e da avaliação da credibilidade da fonte e da qualidade da informação.

O processamento visa o aprimoramento técnico ou a mera viabilização da compreensão da informação. Exemplificativamente, uma conversa entre autoridades estrangeiras precisará ser traduzida, um *e-mail* criptografado demandará decifração, uma fotografia de uma pessoa desconhecida exigirá reconhecimento facial, uma imagem formada por radiação infravermelha será melhor compreendida se convertida em uma ilustração digital. Da mesma forma, uma imagem estática que evidencie uma base de mísseis balísticos não permite concluir, sem que se recorra a um estudo especializado de elementos da imagem, qual o alcance dos mísseis ou mesmo se a base está ou não em atividade. Um especialista em balística, ao analisar a imagem, poderá reconhecer o modelo do míssil e extrair algumas conclusões a respeito de seu alcance. Sinais de marcas de veículos poderão indicar movimento recente na instalação. Da mesma forma, a interceptação de uma conversa telefônica poderá revelar planejamentos terroristas, mas apenas procedimentos de rastreamento da comunicação possibilitarão desvendar a localização dos interlocutores, viabilizando assim sua prisão.

Já a avaliação é a tarefa que tem por objetivo aferir: a) a credibilidade da fonte e b) a qualidade da informação.

Ainda que a definição da credibilidade da fonte se aplique tanto àquelas humanas e não-humanas (é possível que uma fonte técnica esteja recebendo dados falsos em uma operação de engano), o grande desafio para os serviços de inteligência é saber se um entrevistado ou um informante está ou não mentindo; em outras palavras, qual é o valor da informação que essa pessoa fornece. Para tanto, busca-se investigar sua vida pregressa, a posição que ocupa, a exatidão de seus conhecimentos a respeito do assunto sobre o qual é entrevistada, os eventuais motivos que teria ela para mentir ou dizer a verdade e até mesmo a forma como

responde às indagações, se hesitante ou não, além da realização do teste do polígrafo.⁹⁸

A inteligência militar do exército dos Estados Unidos estabelece um mecanismo de *ratings* para a classificação das fontes em seis níveis de confiabilidade (A-F):

Avaliação da Confiabilidade da Fonte

A	Confiável	Não há dúvida da autenticidade, confiabilidade, ou competência; tem um histórico de confiabilidade completa.
B	Usualmente confiável	Poucas dúvidas sobre a autenticidade, confiabilidade, ou competência; tem um histórico de informação válida a maior parte do tempo.
C	Razoavelmente confiável	Dúvidas sobre a autenticidade, confiabilidade, ou competência, mas forneceu informações válidas no passado.
D	Não usualmente confiável	Dúvida significativa sobre a autenticidade, confiabilidade, ou competência, mas forneceu informações válidas no passado.
E	Não confiável	Ausência de autenticidade, confiabilidade, e competência; histórico de informações inválidas.
F	Não se pode determinar	Não existe base para avaliar a confiabilidade da fonte.

(Adaptado de UNITED STATES DEPARTMENT OF THE ARMY HEADQUARTERS. **FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations**, sept. 2006. Appendix B: Source and Information Reliability Matrix, B-1).

Não necessariamente uma fonte confiável fornecerá uma informação verdadeira. Pode ser que a fonte se equivoque, ainda que de boa-fé, a respeito de determinada informação ou mesmo forneça informações falsas que acredite serem verdadeiras. Logo, além de avaliar a confiabilidade da fonte, é necessário também apurar a qualidade da informação.

Como observa Glenn Hastedt, esta qualidade pode ser aferida na medida em que existam outras informações anteriormente coletadas que são consistentes com a que se avalia, formando assim um conjunto coerente e, portanto, mais verossímil.

⁹⁸ Para um estudo compreensivo sobre as evidências científicas de eficácia do exame poligráfico conferir: NELSON, Raymond. Scientific Basis for Polygraph Testing. **Polygraph**, v. 44, n. 1, 2015. Disponível em: https://apoa.memberclicks.net/assets/docs/nelson_2015_scientific_basis_for_polygraph.pdf

Quando diversas fontes fornecerem a mesma informação, a chance de ser ela verdadeira é, da mesma forma, maior.⁹⁹

O exército estadunidense estabelece um ranqueamento de seis níveis (1-6) para avaliar também o conteúdo da informação, de acordo com a matriz abaixo:

Avaliação do Conteúdo da Informação

1	Confirmada	Confirmada por outras fontes independentes; lógica em si mesma; consistente com outra informação sobre o assunto.
2	Provavelmente verdadeira	Não confirmada; lógica em si mesma; consistente com outra informação sobre o assunto.
3	Possivelmente verdadeira	Não confirmada; razoavelmente lógica em si mesma; coerente com algumas outras informações sobre o assunto.
4	Duvidosamente verdadeira	Não confirmada; possível mas não lógica ; nenhuma outra informação sobre o assunto .
5	Improvável	Não confirmada; não lógica em si mesma; contraditada por outras informações sobre o assunto.
6	Não se pode determinar	Não existe base para avaliar a validade da informação.

(Adaptado de UNITED STATES DEPARTMENT OF THE ARMY HEADQUARTERS. *op. cit.* Appendix B-2).

1.2.4 A atividade de análise de informações

A informação “bruta” coletada é apenas uma constatação de um dado da realidade. Um relato de um informante, uma conversa telefônica, imagens de satélite, sinais de radares, um *e-mail*, são somente a representação de um evento passado ou de uma situação presente. Um simples e imediato contato com a informação geralmente não possibilita compreender o que ela significa e quais serão suas implicações. Diante de um emaranhado de informações coletadas em um fluxo ininterrupto, podendo ocorrer que a princípio não haja qualquer conexão entre elas, a tarefa do analista é a de “ligar os pontos”: correlacionar informações, avaliar sua credibilidade, identificar seu significado e suas potencialidades. Como reconheceu o

⁹⁹ HASTEDT, G. *op cit.* p. 53.

ex-Presidente estadunidense Ronald Reagan, “Não é suficiente, obviamente, apenas coletar informação. Análise detida é vital para o bom processo decisório”.¹⁰⁰

A relação entre a coleta e a análise não é uma simples “via de mão única” de fornecimento. Como discutido na seção 1.2.1, não só o processo de requisição orienta a coleta, pois analistas, que são os destinatários imediatos da informação coletada, podem sugerir a busca por aquelas que são necessárias para a melhor compreensão de determinada questão.¹⁰¹

O papel do analista é prover os “consumidores” com avaliações imparciais e objetivas. Nisso se concentram os principais desafios da análise. A imparcialidade exige do analista superar qualquer orientação ideológica e partidária em seus relatórios. Como afirma John Hollister Hedley, “Analistas devem deixar suas opiniões políticas à porta. Objetividade é a palavra-chave do analista; honestidade intelectual seu valor central”.¹⁰² Com efeito, um relatório objetivo é aquele cuja análise é fundamentada em evidências fáticas, evitando especulações e deduções. Como advertia a CIA em seu *Compendium of Analytical Tradecraft Notes*: “Quanto maior a dependência do analista em seu julgamento ao invés de evidências; então maior a probabilidade de erro de estimativa”.¹⁰³

Para ilustrar a atividade da análise, recorre-se a interessante exemplo de um relatório *top secret* da CIA no qual se busca correlacionar eventos e extrair possíveis consequências a respeito do conflito étnico de Ruanda em 1994. Seguindo a derrubada do avião que transportava o então presidente hutu Juvénal Habyarimana e o então presidente do Burundi, Cyprien Ntaryamira, de retorno à celebração do Acordo de Paz de Arusha em 06 de abril de 1994 – evento que engatilhou o genocídio de Ruanda – avaliou um analista da CIA já no dia seguinte:

“Mortes Presidenciais Devem Fazer Reiniciar o Conflito – O Presidente de Ruanda Habyarimana e o Presidente de Burundi Nyaryamira (sic) foram mortos quando seu avião foi alegadamente

¹⁰⁰ “It is not enough, of course, simply to collect information. Thoughtful analysis is vital to sound decisionmaking (sic)”. CENTRAL INTELLIGENCE AGENCY. **Our First Line of Defense: Presidential Reflections on US Intelligence**, Center for the Study of Intelligence 1996. p. 47.

¹⁰¹ HEDLEY, John Hollister. The Challenges of Intelligence Analysis. In JOHNSON, Loch K. **Strategic...** op cit. v.1. p. 128.

¹⁰² “Analysts must check their personal political views at the door. Objectivity is the analyst’s by-word, intellectual honesty the core value”. HEDLEY, John Hollister. The Challenges of Intelligence Analysis. In JOHNSON, Loch K. **Strategic...** op cit. v.1. p. 128.

¹⁰³ “The greater the analysts’ reliance on judgment rather than evidence; thus the greater the likelihood of estimative error”. CENTRAL INTELLIGENCE AGENCY **A Compendium of Analytic Tradecraft Notes**, v. 1, 1997. p. 9.

atacado quando pousou em Kigali na noite passada. Os dois homens, ambos da etnia Hutu, estavam retornando das negociações de paz mediada pela Tanzânia para pôr fim ao conflito étnico na região. **Como os hutus em Ruanda buscam vingança contra os Tutsis, a guerra civil deve recomeçar e ramificar para o vizinho Burundi. O exército tutsi do Burundi, que mantém uma desconfortável trégua com o governo hutu, provavelmente irá tentar tomar o poder**".¹⁰⁴

Hoje pode-se dizer que o prognóstico traçado pelo analista estava correto: de fato a morte dos presidentes engatilhou o reinício da guerra civil e o genocídio de cerca de oitocentos mil tutsis e hutus moderados em Ruanda. Em Burundi, de fato ocorreu um golpe militar de Estado em 1996, quando o exército depôs o presidente hutu Sylvestre Ntibantunganya, fazendo retornar ao posto o tutsi Pierre Buyoya e lançando o país em uma nova onda de violência.¹⁰⁵

Obviamente, a atividade de análise não deve se converter em um frágil exercício de futurologia. Como dito anteriormente, qualquer avaliação deve ser feita com base em evidências concretas. Asserções formuladas ao redor de juízos de probabilidade devem ser claramente relatadas como tal. A propósito, lembra Michael Herman que Robert Gates, um ex-diretor da CIA, dividia as demandas dos “consumidores” em duas categorias: segredos e mistérios. “Segredos” seriam informações potencialmente coletáveis ao passo que “mistérios” seriam respostas inatingíveis, normalmente porque os outros líderes ainda não sabem eles próprios como irão decidir determinada questão.¹⁰⁶

Um clássico exemplo de erro de avaliação foi a crença dominante entre os analistas estadunidenses durante a guerra fria de que o então líder soviético Nikita Khrushchev iria racionalmente optar por não enviar mísseis para Cuba. De fato, a opção por enviar os mísseis se revelou desastrosa do ponto de vista político, e sua

¹⁰⁴ ***“Presidential Deaths Likely to Renew Fighting – Rwandan President Habyarimana and Burundian President Nyaryamira (sic) were killed when their plane was reportedly fired on as it landed in Kigali last night. The two men, both ethnic Hutus, were returning from Tanzanian-sponsored peace talks to end ethnic fighting in the region. As hutus in Rwanda seek revenge on Tutsis, the civil war may resume and could spill over to neighboring Burundi. Burundi’s Tutsi-dominated military, which has an uneasy truce with the Hutu-dominated government, will probably try to take power”.*** CENTRAL INTELLIGENCE AGENCY. *National Intelligence Daily*, 7 april 1994. p. 12. Disponível em: <http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000638200.pdf>

¹⁰⁵ 6,000 Reported Killed in Burundi Coup. **The New York Times**, 23 ago. 1996. Disponível em: <<http://www.nytimes.com/1996/08/23/world/6000-reported-killed-in-burundi-coup.html>>

¹⁰⁶ HERMAN, M. *op. cit.* p. 103.

retirada foi um dos fatores que contribuíram para o declínio de Khrushchev. Por outro lado, como pontua John Hollister Hedley, o equívoco dos analistas norte-americanos

[...] demonstra a necessidade de ser cético a respeito de um modelo de “ator racional”. O líder soviético não via a equação de risco da mesma forma. No final, foi nossa insuficiente compreensão da sua psicologia e visão de mundo que nos levou a acreditar que o ato de enviar os mísseis seria uma opção irracional.¹⁰⁷

Se o erro de avaliação dos analistas na oportunidade da crise dos mísseis não resultou em consequências mais trágicas, há situações em que falhas de análise conduzem a drásticas decisões de Estado. Talvez o exemplo mais claro seja a invasão militar do Iraque em 2003, motivada pela conclusão errônea da inteligência norte-americana de que o regime de Saddam Hussein ocultava armas químicas no território iraquiano (conferir **Anexo 1**). Quando o então Secretário de Estado Colin Powell fez o fatídico discurso perante o Conselho de Segurança da ONU, buscando autorização para utilização da força, foi acompanhado pelo diretor da CIA George Tenet, em claro sinal de suporte da inteligência à invasão.¹⁰⁸

¹⁰⁷ “*But the analysts’ misjudgment points up the need to be skeptical of a “rational actor” model. The Soviet leader did not see the risk equation in the same way. In the end, it was our insufficient understanding of his psychology and world view that led us to believe the act of sending the missiles would be an irrational option*”. HEDLEY, J. H. The Challenges of Intelligence Analysis. In: JOHNSON, L. K. **Strategic**... *op cit.* p. 134.

¹⁰⁸ O discurso completo de Collin Powell no Conselho de Segurança da ONU pode ser assistido em: [FULL] Colin Powell's Presentation to the UN Security Council on Iraq's WMD Program. **Youtube**, Disponível em: <<https://www.youtube.com/watch?v=ErIDSJHRVMA>>



(Tenet e Powell, Conselho de Segurança, 05 fevereiro de 2003. Créditos da Imagem: AP/Wide World Photos. Fonte: PILLAR, Paul R. Intelligence, Policy and the War in Iraq. *Foreign Affairs*, v. 85, n. 2, mar/abr. 2006.)

As “provas” apresentadas ao Conselho no momento, dentre elas imagens de caminhões que supostamente guarneciam unidades móveis de fabricação de armas biológicas, hoje se sabe¹⁰⁹, não iam além de informações não confirmadas repassadas por fontes não confiáveis, sustentadas principalmente nos relatos de um refugiado iraquiano sob custódia do *BND* em Munique, a quem ironicamente foi atribuído o codinome de *curveball*¹¹⁰ e nunca diretamente interrogado pela inteligência dos Estados Unidos.¹¹¹ O fracasso colossal em encontrar qualquer arma

¹⁰⁹ Se hoje se tem uma boa noção a respeito das falhas de inteligência que formaram a crença da existência de armas biológicas ocultas no Iraque, a Comissão de Monitoração, Verificação e Inspeção da ONU, chefiada pelo sueco Hans Blix, já relatava ao Conselho de Segurança conclusão contrária em fevereiro de 2003, após mais de 400 inspeções em mais de 300 locais. Cf. HANS Blix Briefing to the Security Council. *The Guardian*, 14 fev. 2003. Disponível em: <<http://www.theguardian.com/world/2003/feb/14/iraq.unitednations1>>

¹¹⁰ A expressão vem do *Baseball*, e se refere a um lançamento em que se atribui efeito à bola com o intuito de confundir o rebatedor. Uma excelente investigação jornalística sobre o papel de *curveball* e das falhas de inteligência que culminaram com a invasão do Iraque em 2003, pode ser lida em: DROGIN, Bob. *Curveball*. Tradução: Ricardo Gozzi. São Paulo: Novo Conceito, 2008.

¹¹¹ É também oficial a conclusão que destaca a indevida importância que a inteligência dos Estados Unidos conferiu aos relatos do refugiado iraquiano: “One of the most painful errors, however, concerned Iraq’s biological weapons programs. Virtually all of the Intelligence Community’s information on Iraq’s alleged mobile biological weapons facilities was supplied by a source, codenamed “Curveball,” who was a fabricator. THE COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION.

biológica durante a ocupação do Iraque fez acentuar falhas grosseiras na inteligência do país, reconhecidas oficialmente por uma comissão especialmente designada para avaliar as capacidades da inteligência dos Estados Unidos no que diz respeito a armas de destruição em massa.¹¹² Como resultado, um revés político histórico para o governo republicano de George W. Bush e para o *premier* britânico Tony Blair por ter aliado o Reino Unido à campanha militar.¹¹³

O fato é que, qualquer que seja o nível de segurança que se tenha com afirmações formuladas em determinado relatório de análise, é da natureza da atividade a sujeição a erros. Seja ela qual for, uma análise precisa ser feita: cenários avaliados, prognósticos de riscos desenhados, consequências políticas consideradas. Dessa forma, o analista precisa assumir riscos para produzir algo que exceda conclusões absolutamente evidentes e óbvias, que são de todo inúteis para a inteligência de Estado. O que se pode, e deve, sempre ter como norte é minimizar as chances de erro.

1.2.5 A atividade de disseminação de informações

Uma vez processada pela análise, a informação estará qualificada para ser disseminada às autoridades estatais a quem possa interessar, os chamados “consumidores” ou “clientes” da inteligência, normalmente autoridades políticas e militares de alto-escalão.

Nota-se que são várias as formas pelas quais o produto da análise é disseminado, aqui recorrendo-se mais uma vez ao exemplo dos Estados Unidos para ilustrar tal procedimento com três variantes:¹¹⁴

Report to the President of the United States, 31 mar. 2005. p. 48. Disponível em: <https://fas.org/irp/offdocs/wmd_report.pdf>

¹¹² Uma passagem da versão não-classificada do documento é incisiva sobre a falha de inteligência: “*The Intelligence Community’s performance in assessing Iraq’s pre-war weapons of mass destruction programs was a major intelligence failure. The failure was not merely that the Intelligence Community’s assessments were wrong. There were also serious shortcomings in the way these assessments were made and communicated to policymakers*”. THE COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION. *op. cit.* p. 46. Disponível em: <https://fas.org/irp/offdocs/wmd_report.pdf>

¹¹³ Ainda assim há quem defenda o argumento de que a invasão do Iraque em 2003 foi lícita de acordo com o Direito Internacional. Cf. YOO, John. **The Powers of War and Peace: The Constitution and Foreign Affairs after 9/11**. The University of Chicago Press, 2005. p. 170-171.

¹¹⁴ Todos eles retirados de: HEDLEY, J. H. Analysis for strategic intelligence. In: JOHNSON, L. K. **Handbook...** *op. cit.* p. 214.

- Inteligência atual (*current intelligence*)¹¹⁵: é o resultado do trabalho cotidiano das agências de inteligência. Normalmente assumindo a forma de breves relatórios ou de memorandos que são dirigidos diariamente às autoridades ou então sob requisição feita para atender a demandas específicas por análises (*actionable intelligence*). Quando destinada ao Presidente, é chamada de “Informativo Diário do Presidente” (*President’s Daily Briefing – PDB*) e é normalmente reportada de forma oral em reunião matinal com o Chefe de Estado. O Presidente Bill Clinton, diversamente, dispensava a reunião, preferindo ler o relatório de cerca de seis páginas elaborado diariamente pela CIA.¹¹⁶ [conferir um exemplo de um *President’s Daily Briefing* no **Anexo 2**].
- Inteligência básica (*basic intelligence*): trata-se do conhecimento acumulado dos serviços de inteligência, condensado em suas extensas bases de dados. Reúne informações detalhadas sobre indivíduos, e dados geográficos, políticos, econômicos, sociais e militares de países, organizados em formas de monografias, mapas, gráficos e outros tipos de estudos. A CIA, por exemplo, disponibiliza *online* anual e publicamente sua versão do *World Factbook*: um compilado de informações sobre 267 países e outras entidades no mundo.¹¹⁷ Dessa forma, parte da inteligência básica é publicamente acessível e o que for classificado poderá ser conhecido pelas autoridades políticas de acordo com o nível de suas credenciais de segurança (ler nos próximos parágrafos sobre mecanismo de classificação de informações).
- Estimativa de Inteligência Nacional (*National Intelligence Estimate – NIE*): consiste no mais importante produto da inteligência estadunidense pois resume previsões conjugadas das 17 agências de inteligência do país, através da coordenação do *National Intelligence Council*. Sua função é fornecer orientação estratégica para a política externa, normalmente com foco em três a cinco anos a frente. (conferir **Anexo 1**)
- Inteligência de alerta (*warning intelligence*): Disseminada em caráter de urgência, trata-se de informação destinada a acionar uma resposta imediata ou a curto prazo do governo, normalmente de mobilização de forças

¹¹⁵ Apesar de ter se optado nesta tese por utilizar a expressão “informação” em vez de “inteligência” para designar o produto do trabalho das agências (cf. seção II da Metodologia, “Parâmetros conceituais”), aqui não se observou essa técnica por respeito à tradução.

¹¹⁶ DROGIN, B. *op. cit.* p. 254.

¹¹⁷ CENTRAL INTELLIGENCE AGENCY. **The World Factbook**. Disponível em: <<https://www.cia.gov/library/publications/the-world-factbook/>>

armadas.¹¹⁸ Nos Estados Unidos as agências de inteligência cooperam o sistema CRITIC, que possibilita o alerta simultâneo do Presidente e outros oficiais em poucos minutos sobre questões que possam afetar a segurança do país ou a deflagração de eventos que possam provocar crises externas.¹¹⁹

Os relatórios de análise, após redigidos, serão inseridos em um sistema de classificação, o que tem por objetivo hierarquizar as informações segundo sua sensibilidade para a segurança nacional. O grau de classificação atribuído a uma informação será então diretamente proporcional à sua relevância para a segurança nacional e inversamente proporcional ao número de pessoas que a ela terão acesso.

Nos Estados Unidos o sistema de classificação é regido pela *Executive Order* nº 13526, assinada pelo ex-presidente Barack Obama em 2009. De acordo com a ordem presidencial, uma informação pode ser classificada como “*Top Secret*”, “*Secret*” ou “*Confidential*”, caso sua divulgação não autorizada possa provocar, respectivamente, dano grave, sério ou ordinário à segurança nacional (Part I, Sec. 1.2., “a”). Havendo dúvidas significantes sobre qual nível de classificação atribuir a determinada informação, atribui-se o menor nível (Sec. 1.2., “c”). Além dos três estratos de classificação, existem ainda os chamados “Programas Especiais de Acesso” (*Special Accesss Program*), que impõem restrições adicionais ao conhecimento de informações de “excepcional vulnerabilidade”, reduzindo o acesso a um grupo “razoavelmente pequeno” de pessoas. (Sec. 4.3).

A autoridade para classificar originalmente informações no país reside no a) Presidente e Vice-Presidente; b) Chefes das agências e oficiais designados pelo Presidente e c) oficiais do governo a quem foi delegada tal autoridade. (Sec. 1.3).

No Brasil, a chamada “Lei de Acesso à Informação” (Lei 12.527/2011) regulamenta o procedimento de classificação, estabelecendo os níveis “Ultrassegredo”, “Segredo” e “Reservado”. (art. 24). As autoridades que detêm competência para classificar uma informação no nível máximo, ou seja, o ultrassegredo, são: a) Presidente da República; b) Vice-Presidente da República; c) Ministros de Estado e autoridades com as mesmas prerrogativas; d) Comandantes

¹¹⁸ JOHNSON, L. K. **Strategic...** *op. cit.*, v. 2. Appendix D: Categories of Finished Intelligence and the Major Products, p. 239.

¹¹⁹ Alguns comentários sobre o sistema CRITIC podem ser lidos no documento desclassificado: CENTRAL INTELLIGENCE AGENCY. **Notes on the Critic System**. Disponível em: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol4no2/html/v04i2a03p_0001.htm>

da Marinha, do Exército e da Aeronáutica; e e) Chefes de Missões Diplomáticas e Consulares permanentes no exterior. (art. 27, inciso I).

O procedimento de classificação ainda define o prazo durante o qual a informação será sigilosa. No Brasil, o prazo máximo de restrição da informação ultrassecreta é de 25 anos, da secreta 15 anos e da reservada 5 anos, todos contados a partir da data da produção da informação (art. 24, §1º, Lei 12.527/2011), ou, alternativamente, define-se a ocorrência de um evento como termo final do sigilo (art. 24, §3º). Terminado o prazo ou consumado o evento que defina o seu termo final, a informação automaticamente se torna “de acesso público” (§ 4º).

Nos Estados Unidos, não existem prazos legais prévios de classificação. Não obstante, em regra, o sigilo da informação classificada no país não excede 25 anos (*Executive Order nº 13526*, sec. 1.5), havendo nove exceções que permitem que seja esse prazo estendido (sec. 3.3).

Definir quem tem acesso à informação classificada é, obviamente, questão diversa de se definir quem tem competência para a classificação, e é matéria normalmente regulamentada por atos normativos do executivo.¹²⁰ Em regra, uma pessoa com credenciais de segurança (*security clearance*) para acessar uma informação de determinado nível poderá também acessar as informações dos estratos de classificação inferiores. Por outro lado, nos Estados Unidos é possível que existam requisitos adicionais de acesso, de forma que, exemplificativamente, uma pessoa com credenciais *top secret* normalmente não poderá acessar todas as informações desse nível, sendo necessário demonstrar uma necessidade por conhecer (*need-to-know*) a informação em razão de sua função. (*Executive Order nº 13526*, Sec. 4.1, “3”).

Analisando a questão sob um aspecto mais teórico, com foco na relação entre a inteligência e a dimensão política, nota-se que a atividade de análise e de processamento que precedem a tarefa da disseminação faz com que esta etapa não consista em uma simples distribuição de informações da inteligência para o meio político. Trata-se de algo mais substancial. O que é disseminado é o produto de um processo de qualificação de informações, o que é diferente da informação meramente coletada. Por essa razão, é preciso evitar que a informação seja

¹²⁰ No Brasil a matéria é regulamentada pelo Decreto 7.845/2012, competindo ao Núcleo de Segurança e Credenciamento, órgão central de credenciamento de segurança, instituído no âmbito do Gabinete de Segurança Institucional da Presidência da República, habilitar outros órgãos para expedir credenciais de acesso.

repassada diretamente da coleta para as autoridades políticas, caso em que importantes decisões poderiam se sustentar em dados vagos e imprecisos, ou mesmo falsos ou serem enviesadas por opiniões pessoais ante a ausência de uma análise profissional.

Com efeito, nos dizeres de Peter Gill, políticos ávidos por decidir, escolher um rumo de ação, podem não querer esperar enquanto oficiais de inteligência contemplam as nuances de sua análise. Se creem que a informação que detêm, seus contatos, e suas avaliações são ao menos tão bons quanto os da inteligência, há grandes chances de que suas políticas sejam influenciadas por suas próprias crenças, ideologias e percepções.¹²¹ Apesar disso não ser necessariamente um problema, o será se a decisão política contrariar sensivelmente uma orientação da inteligência que posteriormente se revele mais adequada, situação que exigirá explicações da autoridade política da razão por ter ignorado o julgamento da análise. Um bom exemplo disso ocorreu na gestão de George W. Bush quando foram subestimados relatórios da *CIA* que alertavam para a iminência de um ataque terrorista em solo norte-americano no ano de 2001. (cf. capítulo 2).

Pode ocorrer também que políticos sejam acometidos por um ímpeto de pressionar, ainda que de forma sutil, analistas e gestores de agências de inteligência para produzirem estimativas que corroborem suas políticas atuais.¹²² Se, por um lado, a conclusão de que o regime de Saddam Hussein ocultava armas de destruição em massa em 2003 foi um grave erro de análise, por outro, havia grande pressão política ao momento para que a inteligência apoiasse, ao que tudo indica, uma predisposição já sólida nos escalões mais altos da administração à invasão do Iraque. O Oficial de Inteligência sênior dos Estados Unidos para o Oriente Próximo e o Sul da Ásia entre os anos de 2000 e 2005, Paul R. Pillar, afirmou categoricamente: “A administração [Bush] usou a inteligência não para orientar o processo decisório, mas para justificar uma decisão já tomada”.¹²³

Diante de situações como esta, de promíscua relação entre a inteligência e a política, se discute, há algum tempo, quão estreito deve ser o vínculo entre essas duas dimensões. Há duas posições a respeito. Um primeiro argumento, sustentado

¹²¹ GILL, Peter. Sorting The Wood From The Trees: Were 9/11 And Iraq “Intelligence Failures”? In: JOHNSON, L. K. **Strategic**... *op. cit.* p. 153.

¹²² WIRTZ, James J. The Intelligence-Policy Nexus. In: JOHNSON, L. K. **Strategic**... *op. cit.* p. 139.

¹²³ “The administration used intelligence not to inform decision-making, but to justify a decision already made”. PILLAR, Paul R. Intelligence, Policy and the War in Iraq. **Foreign Affairs**, v. 85, n. 2, mar/abr. 2006. p. 17-18.

principalmente pelo historiador Sherman Kent, quem contribuiu decisivamente para a formação da comunidade de inteligência dos Estados Unidos no pós-segunda guerra mundial, se orientava pela ideia de que, para ser eficaz, uma agência de inteligência precisa ser independente. A fim de evitar politização, gestores e analistas de inteligência não deveriam se envolver com autoridades políticas e nem delas receber exigências pontuais, valendo-se de liberdade intelectual para coletar e analisar as informações segundo balizas suficientemente amplas a lhes permitir grande margem de autonomia.¹²⁴ A ideia central por trás desse argumento, como se nota, é evitar que autoridades submetam a inteligência a objetivos políticos individuais, muitas vezes eleitorais, solicitando informações específicas que servirão apenas para justificar publicamente decisões que já foram tomadas nos bastidores, e não orientando a tomada de decisões, que é a real finalidade do serviço de inteligência. Por outro lado, o modelo de Sherman Kent possui o risco de criar barreiras tais que afastem a inteligência e a política em um nível prejudicial, que ocorrerá na medida em que oficiais de inteligência não consigam perceber as reais demandas dos tomadores de decisão. Se a comunicação de um serviço de inteligência com as autoridades políticas for reduzida a essa condição, provavelmente seus relatórios não cobrirão as questões que efetivamente precisam ser decididas politicamente ou, ainda se o fizer, não possuirão o nível de detalhamento adequado.¹²⁵

Esse modelo orientou a organização da CIA até a década de 1980, quando Robert Gates assumiu o cargo de Diretor Assistente da agência (*deputy director*). Em sua gestão, Gates criou o mecanismo de “inteligência acionável” (*actionable intelligence*) para suprir demandas específicas de oficiais da administração pública por informações. O procedimento faria com que, segundo ele, os analistas se tornassem menos “acadêmicos” e mais atentos às necessidades dos “consumidores”, portanto, capazes de produzir análises mais relevantes e atualizadas.¹²⁶ Gates argumenta que o oficial de inteligência deve efetivamente trabalhar em conjunto com a autoridade política, conhecer suas preocupações atuais e futuras e mesmo suas opiniões a respeito de temas que influenciem na análise. Da mesma forma, uma adoção radical desse modelo poderia resultar no enviesamento

¹²⁴ WIRTZ, J. *op. cit.* p. 141.

¹²⁵ *Ibidem.* p. 142.

¹²⁶ *Ibidem.* p. 142.

político das questões formuladas pelos “consumidores”, garantindo análises favoráveis à sua política.¹²⁷

Como se pode concluir, um ponto ótimo para a relação inteligência-política reside à meia distância entre os dois modelos descritos ou, se poderia dizer, em uma conjugação dos pontos fortes de cada um. De um lado, é preciso preservar a independência do serviço de inteligência, o que pode ser atingido através do fomento a uma cultura de profissionalismo no âmbito das agências. Não se trata de blindar o oficial de inteligência contra pressões políticas externas – algo impossível – mas sim de conferir garantias, tanto práticas quanto legais¹²⁸, de que seu trabalho poderá ser exercido sem temor de represálias. Dessa forma, o profissional da inteligência poderá e deverá relatar informações de forma objetiva e verdadeira. Nessa tarefa, vale dizer, ao redigir um relatório de análise destinado a uma autoridade política, o analista deve se acautelar de que a tarefa da inteligência não é decidir pelo político mas sim apresentar opções e esclarecer suas consequências. Como explica John Hollister Hedley:

Como a análise informa a política? Com muito cuidado. Tem-se dito que para que analistas colaborem com autoridades políticas de forma relevante se mantendo absolutamente neutros do ponto de vista político é como tentar nadar sem se molhar. Analistas devem trilhar um caminho delicado se sua análise não deve ser prescritiva. De alguma forma eles devem iluminar alternativas sem sugerir qual delas escolher.¹²⁹

Concomitantemente, uma vez garantida a independência do profissional de inteligência, é possível manter uma proximidade tal com os “consumidores” que se

¹²⁷ *Ibidem*. p. 143. Esse risco existe na medida em que se sabe, por comprovação científica, que mesmo a forma como uma pergunta é formulada pode influenciar na resposta. Em estudos de economia comportamental, esse resultado é conhecido como *framing effects*, já observado em diversas pesquisas científicas. Para uma descrição compreensiva desse efeito conferir: HANSON, Jon D.; KYSAR, Douglas A. Taking Behavioralism Seriously: The Problem of Market Manipulation. **New York University Law Review**, v. 74, 2008. p. 154-156.

¹²⁸ A CIA, por exemplo, encarrega um *ombudsman* com competência para ouvir reclamações e iniciar inquéritos sobre tentativas de politização sobre o trabalho de seus profissionais, figura criada na agência pelo próprio Robert Gates em 1992. GATES, Robert. **Guarding Against Politicization: a message to analysts**, 16 mar. 1992. Disponível em: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/volume-36-number-1/html/v36i1a01p_0001.htm>

¹²⁹ “How analysis informs policy might be answered with “very carefully.” It has been said that for analysts to collaborate with policymakers in the interest of relevance while remaining absolutely policy-neutral is like trying to swim without getting wet. Analysts must walk a fine line if their analysis is not to be prescriptive. Somehow they must illuminate alternatives without suggesting which one to take”. HEDLEY, J. H. Analysis for strategic intelligence. In: JOHNSON, L. K. **Handbook**... *op. cit.* p. 219.

possa ter uma noção clara de quais preocupações são as mais relevantes para sua tomada de decisão, sem que com isso esteja ele sujeito a ingerências políticas.

1.3 Como a atividade de inteligência é organizada

Normalmente, os Estados possuem sistemas de inteligência que são organizados tanto em agências especializadas no exercício da atividade quanto em divisões integradas a órgãos que não tem por finalidade principal tarefas de inteligência, mas o fazem de forma acessória. Um exemplo dessa última hipótese seria o escritório de inteligência do Departamento do Tesouro dos Estados Unidos, como se verá adiante. É comum ainda que o serviço de inteligência estatal se divida em agências incumbidas da inteligência externa (ex: *CIA*, *Mossad*) ao lado de agências que realizam inteligência interna com finalidades de segurança. São exemplos de agências de inteligência de segurança o *FBI*, o *Canadian Security Intelligence Service (CSIS)*, a *Direction de la Surveillance du Territoire (DST)* francesa, o *Bundesamt für Verfassungsschutz (BfV)* alemão e o *Sherut ha'Bitachon ha'Klali (Shin Bet)* israelense.¹³⁰

Para que se possa compreender com maior exatidão o quão complexa pode ser a estrutura de um sistema de inteligência estatal, vale ser analisada a comunidade de inteligência dos Estados Unidos¹³¹, que é composta de 17 agências e órgãos atuando de forma independente e cooperativa¹³², com um orçamento anual de cerca de US\$ 67 bilhões de dólares.¹³³

¹³⁰ CEPIK, Marco. Sistemas Nacionais de Inteligência: Origens, Lógica de Expansão e Configuração Atual. **DADOS – Revista de Ciências Sociais**, v. 46, n. 1, 2003. p. 93.

¹³¹ Concluir que a estrutura da comunidade de inteligência dos Estados Unidos é complexa não prescinde de um estudo complexo sobre o tema. De fato, não se pode saber com exatidão como cada uma das 17 agências que a compõem operam, naturalmente em razão do sigilo de tais informações. Mesmo ex-funcionários das agências estão obrigados por termos de confidencialidade a não revelar informações de natureza classificada. Portanto, a descrição que se segue será limitada por tais obstáculos.

¹³² Um breve resumo com informações sobre os órgãos que compõem a comunidade de inteligência dos Estados Unidos pode ser lido no *website* do Escritório do Diretor Nacional de Inteligência, e boa parte da descrição das agências apresentadas pode lá ser lido, em: OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE. **Members of the IC**. Disponível em: <<http://www.dni.gov/index.php/intelligence-community/members-of-the-ic>>

¹³³ Esse foi o total apropriado pela comunidade de inteligência dos Estados Unidos no ano de 2014, incluindo a inteligência militar. Já em 2010 o total apropriado foi de cerca de 80 Bilhões de Dólares. Cf. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. **U.S. Intelligence Community Budget**. Disponível em: <<http://www.dni.gov/index.php/resources/intelligence-community-budget>> Trata-se de montante superior ao Produto Interno Bruto de países como a Croácia e o Uruguai por exemplo. A forma como o esse valor é distribuído entre as 17 agências é uma informação classificada, mas sabe-se ser suficiente para pagar os salários de cerca de

i. *Office of the Director of National Intelligence (ODNI)*

O *Office of the Director of National Intelligence* é o órgão central da comunidade de inteligência dos Estados Unidos. Foi criado em reação à percepção de que falhas de cooperação entre as agências de inteligência do país foram uma das causas para a ocorrência dos ataques terroristas de 11 de setembro de 2001. (cf. capítulo 2) Instituiu-se então, como uma das medidas de reforma à comunidade de inteligência do país, o Escritório do Diretor Nacional de Inteligência através do *Intelligence Reform and Terrorism Prevention Act*, de dezembro de 2004.¹³⁴ Tem por principal objetivo coordenar as atividades de coleta e análise das diversas agências e órgãos de inteligência dos Estados Unidos, estabelecendo prioridades estratégicas para emprego dos seus recursos por meio do *National Intelligence Priorities Framework* (cf. seção 1.2.1).

O Diretor Nacional tem acesso a todas informações oriundas dos serviços de inteligência dos Estados Unidos e a atribuição de exercer as mais altas funções de aconselhamento sobre assuntos de inteligência, reportando-se diretamente ao Presidente.¹³⁵

ii. *Central Intelligence Agency (CIA)*

Única agência de inteligência independente na estrutura do executivo estadunidense, a *CIA* é composta por oficiais civis, e é a principal responsável pela condução da inteligência externa dos Estados Unidos. Apesar de não ser a única a conduzir inteligência de fontes humanas (HUMINT), a *CIA* exerce o papel de

100.000 funcionários, programas de lançamento e manutenção de satélites, aeronaves, armas, potentes computadores e diversos outros equipamentos eletrônicos. Um histórico do orçamento da inteligência dos Estados Unidos, contendo as justificativas orçamentárias de cada agência, pode ser lido em FEDERATION OF AMERICAN SCIENTISTS. **Intelligence Resource Program: Intelligence Budget Data**. Disponível em: <<http://fas.org/irp/budget/>> Não obstante, dentre os documentos vazados por Edward Snowden haviam informações sobre a distribuição do orçamento da comunidade de inteligência para o ano de 2013. Um gráfico com a adaptação dessas informações encontra-se no **Anexo 3** e os originais dos documentos vazados podem ser lidos em: ANDREWS, Wilson; LINDEMAN, Todd. \$ 52.6 Billion: The Black Budget. **The Washington Post**, 29. ago. 2013. Disponível em: <<http://www.washingtonpost.com/wp-srv/special/national/black-budget/>> com dados adicionais em <<http://apps.washingtonpost.com/g/page/national/2013-us-intelligence-budget-additional-resources/421/>>

¹³⁴ UNITED STATES OF AMERICA. **Intelligence Reform and Terrorism Prevention Act**, section 118, Stat. 3638. Disponível em: <<https://www.congress.gov/bill/108th-congress/senate-bill/2845>>

¹³⁵ *Ibidem*.

gerência nacional dessa espécie de atividade, além de ser a única autorizada por lei a conduzir operações encobertas (*covert action*) em tempo de paz, a mando do Presidente.^{136 137} A CIA possui destacada capacidade de conduzir “análises de todas as fontes” (*all-source analysis*), em contraste com outras agências que são tecnicamente especializadas, como por exemplo a *National Geospatial-Intelligence Agency (NGA)*.¹³⁸ (cf. item vi).

A Agência é organizada em cinco diretórios principais¹³⁹: a) O *Diretório de Suporte*, que cuida das tarefas administrativas cotidianas da agência, bem como recursos humanos, financeiros e apoio logístico às operações; b) *Diretório de Operações*, divisão responsável pelo gerenciamento do serviço clandestino nacional, incluindo atividades de coleta de fontes humanas com espiões (chamados de “case officers”¹⁴⁰), e operações encobertas; c) *Diretório de Análise*, d) *Diretório de Ciência e Tecnologia*, que fornece apoio de natureza técnica às demais divisões; e) *Diretório de Inovação Digital*, responsável pela gestão de tecnologia de informação e pela gestão das disciplinas de coleta técnica da agência (*SIGINT* e *IMINT*).

iii. *Defense Intelligence Agency (DIA)*

Vinculada ao Departamento de Defesa dos Estados Unidos, a *DIA*, assim como a *CIA*, possui larga capacidade na condução de operações externas de HUMINT, mas com foco estratégico militar. Produz análises que alcançam desde combatentes em campo a militares de alta-patente e autoridades políticas de defesa nacional. O Diretor da *DIA* é o principal conselheiro do Secretário de Defesa.

¹³⁶ UNITED STATES OF AMERICA. 50 U.S. Code § 3093, (a), (3).

¹³⁷ Inclui-se aqui o programa de ataques com veículos aéreos não tripulados, mais conhecidos como *Drones* que é operado em conjunto pela CIA e pelo *Joint Special Operations Command (JSOC)*, uma divisão do Departamento de Defesa. Cf. SHAH, Naureen. A Move Within the Shadows: Will JSOC's Control of Drones Improve Policy? In: BERGEN, Peter L.; ROTHENBERG, Daniel. **Drone Wars: Transforming Conflict, Law and Policy**. Cambridge University Press, 2015.

¹³⁸ MONJE, Scott. **The Central Intelligence Agency: a documentary history**. Greenwood Press, 2008. p.xxi-xxiii.

¹³⁹ MONJE, S. *op cit.* p. xxiv-xxvi; CENTRAL INTELLIGENCE AGENCY. **Offices of CIA**. Disponível em: <<https://www.cia.gov/offices-of-cia>>

¹⁴⁰ “Case officer” é a expressão do jargão da inteligência empregada ao oficial de inteligência, ou o termo mais técnico para a figura do espião. O indivíduo recrutado pelo case officer, normalmente um cidadão estrangeiro, é chamado de “agente”. Indivíduos que são fontes de informação para operações de HUMINT são chamados de “ativos” (assets). Os “case officers” são designados para uma “base” ou “estação” em território estrangeiro, sendo que uma base é subordinada a uma estação. MONJE, S. *op. cit.* p. xxv.

iv. *National Security Agency (NSA)*

A Agência de Segurança Nacional, também vinculada ao Departamento de Defesa, é a principal responsável pela condução da SIGINT norte-americana. Exerce papel fundamental em tarefas de criptografia e decifração, tradução de comunicações em língua estrangeira, e, ainda, segurança cibernética de outras agências de inteligência e órgãos do governo, evitando que suas informações sejam obtidas por outros Estados. Diz-se ainda ser a maior empregadora de matemáticos dos Estados Unidos, possivelmente do mundo.

v. *Federal Bureau of Investigation (FBI) – Intelligence Branch*

O FBI é ligado ao Departamento de Justiça e realiza atividades de inteligência através do seu *Intelligence Branch*, com foco essencialmente doméstico. É responsável pelas atividades de contrainteligência do país e assume expressivo papel no contraterrorismo.

vi. *National Geospatial-Intelligence Agency (NGA)*

A NGA, vinculada ao Departamento de Defesa, realiza a inteligência geoespacial dos Estados Unidos, relacionada a mapeamento e monitoramento de propriedades físicas e geográficas da superfície global. Não trabalha apenas com a coleta e análise de imagens, valendo-se também de dados de posicionamento global e mesmo radiação eletromagnética. A NGA auxilia não apenas em situações militares, fornecendo informações importantes em operações humanitárias e de manutenção da paz.

vii. *National Reconnaissance Office (NRO)*

Também ligado ao Departamento de Defesa, ao Escritório de Reconhecimento Nacional é atribuída a responsabilidade de projetar, construir, lançar e operar os satélites de inteligência dos Estados Unidos. Sua constelação de satélites é capaz de fornecer não apenas imagens estáticas, mas também fornecer

dados em tempo real de lançamentos de mísseis e explosões nucleares, bem como interceptar comunicações.

viii. *Department of Energy (DOE) – Office of Intelligence and Counterintelligence*

A inteligência do *DOE* está especialmente associada ao rastreamento do estoque global de urânio e outros materiais nucleares, e internamente, à proteção dos laboratórios e da propriedade intelectual associados a energia no país.

ix. *Department of Homeland Security (DHS) – Office of Intelligence and Analysis*

A inteligência do *DHS* coleta e analisa informações que possam levar à identificação e eliminação de ameaças à segurança interna dos Estados Unidos. O faz atuando principalmente em questões de proteção fronteiriça e alfandegária, imigração, incluindo concessão de vistos a estrangeiros e transportes.

x. *Department of State (DOS) – Bureau of Intelligence and Research*

A divisão de inteligência do Departamento de Estado tem como principal função assessorar o Secretário de Estado e a diplomacia norte-americana. É o foro principal do debate sobre questões políticas relacionadas à comunidade de inteligência dos Estados Unidos.

xi. *Department of Treasury (DOT) – Office of Intelligence and Analysis*

O escritório de inteligência do Departamento do Tesouro coleta e analisa informações para o exercício do *law enforcement* em assuntos financeiros. Externamente, auxilia no rastreamento de valores envolvidos com atividades terroristas e comércio ilegal de armas.

xii. Outras agências

As demais agências são militares (com exceção da *DEA*) e possuem divisões de inteligência especialmente criadas para auxiliar no exercício de suas tarefas típicas, razão pela qual limita-se aqui a nomeá-las.

Air Force Intelligence, Surveillance, and Reconnaissance Enterprise (USAF - ISR)

Coast Guard Intelligence

Marine Corps Intelligence

Navy – Office of Naval Intelligence

Army Intelligence (G-2)

Drug Enforcement Administration (DEA) – Intelligence Center

É possível também que os Estados se utilizem de empresas privadas na prestação de serviços terceirizados de inteligência (*intelligence outsourcing*), o que se tornou uma tendência crescente após os ataques de 11 de setembro de 2001. Nos Estados Unidos a prática é bastante comum, onde notáveis exemplos de empresas privadas desenvolvem inteligência sob contrato com o governo, tais como a *GK Sierra*, a *Booz Allen Hamilton* (que empregava Edward Snowden), *IBM*, *Amazon*, *Northrop Grumman*, *Lockheed Martin* e *CACI International*.¹⁴¹

1.3.1 Alguns apontamentos sobre a organização da inteligência brasileira¹⁴²

A organização da inteligência brasileira pode ser descrita historicamente em 3 fases. Um primeiro momento tem início em 1964 com o golpe militar e a criação do Serviço Nacional de Inteligência (SNI). Característica comum de regimes ditatoriais, o aparato de inteligência foi utilizado no período para identificação e repressão interna de dissidentes, sob coordenação militar. Disso resultaram práticas frequentes de torturas, violação de correspondências, grampos de telefones, buscas e prisões

¹⁴¹ Cf. SHORROCK, Tim. U.S. Intelligence is More Privatized than ever before. **The Nation**, 16 set. 2015. Disponível em: <<http://www.thenation.com/article/us-intelligence-is-more-privatized-than-ever-before/>>

¹⁴² Cf. CEPIK, Marco Aurelio; ANTUNES, Priscila. Brazil's New Intelligence System: An Institutional Assessment. **International Journal of Intelligence and Counterintelligence**, v. 16, 2003.

sem o respaldo de mandado judicial e forte censura à imprensa. Especialmente no governo do General Emílio Garrastazú Médici (1968-1974) – quem fora chefe do SNI em 1960 – o Serviço ganha força sob a criação do Sistema Nacional de Segurança Interna, se tornando o centro nervoso da inteligência da Marinha, Exército e Aeronáutica – estes últimos que não tinham um órgão de inteligência até então.

Na gestão do Presidente João Baptista Figueiredo (1979-1985) – quem também fora chefe do SNI antes de assumir a Presidência – o Serviço experimenta nova expansão, com alto grau de autonomia operacional. Os progressivos passos em direção à democratização encontraram forte resistência na comunidade de inteligência.

Um segundo período se inicia no governo democrático de José Sarney (1985-1990) que coincide com os momentos finais da guerra fria no cenário internacional. Mesmo aí a gestão do SNI fica a cargo de militares, com foco prioritário em segurança interna e especial atenção às greves trabalhistas e movimentos de esquerda, ainda considerados “subversivos”. Não obstante, a estrutura do SNI é paulatinamente adaptada à nova realidade, e questões de fiscalização fronteiriça e prevenção à espionagem industrial passam a integrar a agenda da inteligência brasileira.

Em 1990 o SNI é extinto pelo Presidente Fernando Collor – cumprindo uma promessa de campanha eleitoral – dando lugar à Secretaria de Assuntos Estratégicos. Tal fato marca o rompimento entre os braços civil e militar da inteligência brasileira. Apesar da reestruturação, as capacidades da nova Secretaria permanecem em essência as mesmas do predecessor SNI, decaindo posteriormente para um momento de perda gradual de pessoal e recursos.

Por fim, um terceiro período é inaugurado em 1999 com a criação da Agência Brasileira de Inteligência (ABIN), na gestão do Presidente Fernando Henrique Cardoso (1994-2002). Essa fase é marcada por uma maior preocupação do Congresso Nacional com assuntos de inteligência – na verdade, anteriormente o tema era amplamente ignorado pelo poder Legislativo. De fato, pela primeira vez na história do país uma agência de inteligência foi criada por lei (a Lei 9.883/1999) em vez de decretos e medidas provisórias. Isso refletia a orientação de que a nova agência não deveria estar subordinada a interesses partidários e ideológicos do governo.

A própria linguagem utilizada na Lei evidencia um grau de maturidade maior das autoridades brasileiras a respeito da atividade de inteligência de Estado. Ao menos em termos legais, há um rompimento com um modelo de inteligência voltado para vigilância interna da população e identificação de “grupos subversivos”. Como definido no art. 1º, § 2º

“[...] entende-se como inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado”.

Além disso, se exalta como fundamentos da atividade a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana, devendo ser observadas os direitos e garantias individuais previstos na Constituição Federal e em acordos internacionais de que o Brasil seja parte (art. 1º, § 1º) e a fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado (art. 3º parágrafo único).

São definidas como competências da ABIN (art. 4º):

- I - planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República;
- II - planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade;
- III - avaliar as ameaças, internas e externas, à ordem constitucional;
- IV - promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência.

A escolha e nomeação ao cargo de Diretor-Geral da ABIN é ato privativo da Presidência da República, sujeito à aprovação do Senado Federal (art. 11, parágrafo único).

A Lei 9.883/1999 também institui o Sistema Brasileiro de Inteligência (SISBIN), do qual a ABIN é o órgão central. Regulado pelo Decreto 4.376/2002, a lei arrola 19 órgãos que compõem o SISBIN.¹⁴³ Não obstante, a verdadeira extensão do

¹⁴³ Casa Civil da Presidência da República; Secretaria de Governo da Presidência da República; Agência Brasileira de Inteligência; Ministério da Justiça, por meio da Secretaria Nacional de Segurança Pública, da Diretoria de Inteligência Policial do Departamento de Polícia Federal, do Departamento de Polícia Rodoviária Federal, do Departamento Penitenciário Nacional e do

Sistema Brasileiro de Inteligência é na verdade bem mais modesta do que se pretende. A inclusão desses órgãos no sistema não significa que todos eles realizem coleta e análise sistemáticas de informações, mas apenas que eventualmente poderão reunir e repassar informações para a ABIN ou outro órgão integrante.

Nos últimos anos, período de forte turbulência política no Brasil, a organização da inteligência brasileira é marcada por instabilidades e incertezas. Até o ano de 2015 a ABIN era organizada na estrutura do Gabinete de Segurança Institucional da Presidência da República – órgão de controle militar. Atendendo a reivindicações para sujeitar a agência ao controle civil, a coordenação das atividades da inteligência do país foi atribuída à Secretaria de Governo, órgão com *status* de ministério. Todavia, com o afastamento da presidente Dilma Rousseff, o governo de Michel Temer reorganizou a ABIN novamente no âmbito do Gabinete de Segurança Institucional em 2016.

1.4 Como a atividade de inteligência é fiscalizada

A fiscalização da atividade de inteligência tem dois objetivos principais: de um lado pretende assegurar que as agências responsáveis por seu exercício consigam cumprir a tarefa para qual foram designadas. Nesse sentido preocupa-se com a *eficácia* dos serviços de inteligência. Isso envolve verificar se as agências fazem uso eficiente e adequado do dinheiro público, se são capazes de fornecer informações e análises relevantes sobre as demandas das autoridades responsáveis pela tomada de decisão e ainda se conseguem antecipar ameaças à segurança nacional.¹⁴⁴

Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, da Secretaria Nacional de Justiça; Ministério da Defesa, por meio da Subchefia de Inteligência Estratégica, da Assessoria de Inteligência Operacional, da Divisão de Inteligência Estratégico-Militar da Subchefia de Estratégia do Estado-Maior da Armada, do Centro de Inteligência da Marinha, do Centro de Inteligência do Exército, do Centro de Inteligência da Aeronáutica, e do Centro Gestor e Operacional do Sistema de Proteção da Amazônia; Ministério das Relações Exteriores, por meio da Secretaria-Geral de Relações Exteriores e da Coordenação-Geral de Combate aos Ilícitos Transnacionais; Ministério da Fazenda, por meio da Secretaria-Executiva do Conselho de Controle de Atividades Financeiras, da Secretaria da Receita Federal do Brasil e do Banco Central do Brasil; Ministério do Trabalho e Previdência Social; Ministério da Saúde; Casa Militar da Presidência da República; Ministério da Ciência e Tecnologia; Ministério do Meio Ambiente; Ministério da Integração Nacional; Controladoria-Geral da União; Ministério da Agricultura, Pecuária e Abastecimento; Secretaria de Aviação Civil da Presidência da República; Ministério dos Transportes; Ministério de Minas e Energia; e Ministério das Comunicações.

¹⁴⁴ CAPARINI, Marina. Controlling and Overseeing Intelligence Services in Democratic States. In: BORN, Hans; CAPARINI, Marina [orgs.]. **Democratic Control of Intelligence Services**. Ashgate, 2007. p. 9.

Normalmente esse tipo de controle é exercido por parlamentares e no âmbito do poder executivo.

De outro lado, a fiscalização das atividades de inteligência também tem por foco a análise da adequação de seus programas e operações à lei, se são consistentes com padrões democráticos e éticos. Nesse aspecto realiza-se um controle de *legalidade*, sendo o judiciário o âmbito mais adequado para apreciar tal qualidade nos serviços de inteligência.

Ocorre que a fiscalização da atividade de inteligência tem que lidar com a peculiaridade de definir como e até que ponto se deve realizar controle democrático sobre uma função vital ao Estado mas que, por sua própria essência, precisa operar sob sigilo. Por um lado uma transparência absoluta da atividade, se é desejável para outras funções estatais, no caso da inteligência iria comprometer o êxito das operações e, em última análise, colocar em risco a vida de agentes e oficiais infiltrados. Por outro, o sigilo que acoberta a inteligência aliado ao poder de obtenção de informações que a atividade proporciona podem encorajar práticas ilícitas por parte de seus operadores. Portanto, a fiscalização dos órgãos de inteligência deve ser feita com o cuidado de se discriminar o que pode ser tornado público para fins de controle e o que deve ser mantido sob segredo por razões de segurança.

Os Estados com os modelos de fiscalização de inteligência mais evoluídos exercem controle da atividade em uma *dimensão vertical*, que é o conduzido no interior da estrutura hierárquica da própria agência que se fiscaliza, e em uma *dimensão horizontal*, que é o realizado por outro órgão estatal (legislativo, executivo, judiciário). Aceita-se ainda a fiscalização de uma *terceira dimensão*, que é aquela feita por atores internacionais (cortes e organizações internacionais, outros Estados etc.).¹⁴⁵

1.4.1 *Fiscalização interna*

Internamente, as agências de inteligência estabelecem hierarquias e procedimentos de autoridade através dos quais se possibilita algum grau de controle exercido por oficiais de alto-escalão. Na Alemanha, por exemplo, a legislação

¹⁴⁵ A classificação é proposta em: CAPARINI, M. *op. cit.* p. 10.

determina que medidas de segurança sejam implementadas sob a supervisão de um membro da agência que possui qualificações para ocupar um cargo judicial no país. Outros Estados da Europa, como Itália, Sérvia e Bósnia Herzegovina, têm a figura do inspetor-geral internamente aos órgãos de inteligência.¹⁴⁶ Já os Estados Unidos possuem cerca de doze inspetores-gerais distribuídos pela comunidade de inteligência, todos funcionários independentes das respectivas agências que fiscalizam.¹⁴⁷

Externamente, as formas de controle da atividade de inteligência são mais rigorosas e eficientes, e se manifestam de variadas formas, a saber:

1.4.2 *Fiscalização parlamentar*

O controle parlamentar é o principal mecanismo de fiscalização política democrática dos serviços de inteligência, pois permite uma abordagem pluripartidária e abrangente da atividade. Sua importância se revela em quatro principais facetas¹⁴⁸: *primeiro*, serve de fiscalizador dos próprios diretores das agências de inteligência que devem reportar suas atividades aos parlamentares, reduzindo assim a margem para abusos; *segundo*, o órgão parlamentar, na sua função de fiscalização do poder executivo, contribui para conter a chamada “politização das atividades de inteligência” para satisfação de propósitos partidários, o que se mostra especialmente relevante após os problemas de imparcialidade da inteligência dos Estados Unidos na deflagração da Guerra do Iraque em 2003; *terceiro*, na definição da dotação orçamentária do serviço de inteligência, o que de certa forma significa estabelecer alguns limites à sua capacidade operacional e *quarto*, na fiscalização da adequação das operações de inteligência à proteção dos direitos humanos.

O mais comum é que se defina uma comissão parlamentar com competência para fiscalizar toda a atividade de inteligência do país ao invés de se estabelecer um órgão para o controle de cada uma das agências. Assim, nos Estados Unidos há

¹⁴⁶ COUNCIL OF EUROPE. **Democratic and effective oversight of national security services**, 2015. p. 58.

¹⁴⁷ LEIGH, Ian. The accountability of security and intelligence agencies. In: JOHNSON, L. K. **Handbook**... *op. cit.* p. 78.

¹⁴⁸ Todas mencionadas por BORN, Hans. Parliamentary and External Oversight of Intelligence Services. In: BORN, H.; CAPARINI, M. *op. cit.* p. 164.

comitês congressionais de fiscalização da inteligência na *House of Representatives* e no *Senate*.¹⁴⁹ Já no Brasil há a Comissão Mista de Controle das Atividades de Inteligência, de caráter permanente, composta por seis deputados e seis senadores.

Geralmente a competência dos órgãos parlamentares para fiscalização limita-se a apreciar as operações de inteligência *ex post facto*, isto é, depois que elas já se realizaram, o que é o caso da maioria dos Estados europeus.¹⁵⁰ Diversamente, nos Estados Unidos e na Alemanha há mecanismos que obrigam que os comitês de inteligência do Congresso sejam informados de programas e operações particulares antes que sejam executados.¹⁵¹ Essa distinção na extensão da competência de fiscalizar também irá determinar o nível de acesso que os parlamentares terão sobre informações classificadas. Na Romênia e na Letônia, por exemplo, os órgãos de fiscalização parlamentar possuem acesso irrestrito à informação classificada.¹⁵²

É possível ainda que a fiscalização parlamentar seja ampla a ponto de cobrir aspectos políticos e legais, bem como de eficiência das operações de inteligência (exemplos: Estados Unidos, África do Sul, Canadá e Argentina), ou seja restrita à análise de aspectos específicos da atividade.¹⁵³ Por exemplo, na Noruega, a fiscalização parlamentar se limita à análise da proteção dos direitos humanos e ao respeito ao Estado de Direito; no Reino Unido o foco é direcionado apenas à questões políticas e administrativas, mas não cobre a licitude de operações; e na Polônia não se afere a eficiência do serviço de inteligência.¹⁵⁴

1.4.3 *Fiscalização pelo executivo*

Geralmente as agências de inteligência são subordinadas à setores ministeriais mais amplos, como defesa, justiça ou interior ou mesmo sob autoridade direta do chefe do executivo, como ocorre na Turquia e na Romênia. É possível também que a inteligência seja organizada no executivo através de conselhos nacionais, como é o caso da Croácia e da Sérvia.¹⁵⁵ O modelo norte-americano, como já visto, pode ser considerado misto pois é constituído tanto de agências

¹⁴⁹ LEIGH, I. *op. cit.* p. 71.

¹⁵⁰ COUNCIL OF EUROPE. **Democratic...** *op. cit.* p. 43.

¹⁵¹ LEIGH, I. *op. cit.* p. 72.

¹⁵² COUNCIL OF EUROPE. **Democratic...** *op. cit.* p. 44.

¹⁵³ BORN, H. *op. cit.* In: BORN, H.; CAPARINI, M. *op. cit.* p. 169.

¹⁵⁴ *Ibidem.* p. 169.

¹⁵⁵ COUNCIL OF EUROPE. **Democratic...** *op. cit.* p. 57.

independentes, como é o caso da CIA, como de agências subordinadas à departamentos do executivo, como por exemplo a DIA, vinculada ao *Department of Defense*. Já o Mossad israelense (*HaMossad leModi'in uleTafkidim Meyuhadim*), o *Sluzhba Vnezhney Rasvedki* (SVR) russo e o BND estão subordinados diretamente ao Primeiro-Ministro ou ao Presidente, conforme for o caso.¹⁵⁶ No Brasil a ABIN atualmente está ligada ao Gabinete de Segurança Institucional da Presidência da República (cf. seção 1.3.1). Em alguns Estados europeus, como é o caso do Reino Unido e da Holanda, ministros do executivo são responsáveis por autorizar o uso de medidas de vigilância e de operações de busca por palavras-chave de comunicações privadas.¹⁵⁷ Nos Estados Unidos, como já dito na seção 1.3, item ii, a autorização para a realização de ações encobertas é de competência do Presidente, devendo o Congresso ser informado.

Como se nota, a fiscalização realizada pelo executivo pode ser considerada externa apenas no sentido de que se realiza fora da estrutura institucional de determinada agência, na medida em que há participação direta de seus membros no processo da inteligência, seja na requisição de informações ou na autorização de operações específicas. Por essa razão, se argumenta que deve existir uma clara definição de competências entre o chefe da agência de inteligência e o membro do executivo a quem ela está subordinada. Nesse espírito, no Canadá, o *Security Intelligence Service Act* (1985), em seu art. 6 (1), determina que o Diretor do serviço tem o “controle e gestão” das agências “sob direção” do Ministro da Segurança Pública e Emergência. Da mesma forma a legislação da Polônia define uma clara separação entre as competências do Primeiro-Ministro em relação às atividades de inteligência e as dos diretores das agências.¹⁵⁸

Ainda a respeito da relação entre os chefes das agências de inteligência e os ministérios a que estão vinculadas, é importante observar que algumas legislações estabelecem a regra de que determinadas instruções ministeriais devem ser feitas por escrito, exatamente para evitar a politização indevida da atividade com a apresentação de instruções questionáveis do ponto de vista ético e/ou jurídico. O faz por exemplo a legislação canadense (*Canadian Security Intelligence Service Act*

¹⁵⁶ CEPIK, M. *Sistemas Nacionais...* op. cit. p. 86.

¹⁵⁷ COUNCIL OF EUROPE. **Democratic...** op. cit. p. 58.

¹⁵⁸ LEIGH, I. op. cit. p. 69.

1985, 7(1) e (2)), húngara (*Act on the National Security Services*, 1995, seção 11) e australiana (*Intelligence Services Act*, 2001, 8(1)).¹⁵⁹

No Brasil há interessante disposição na legislação que determina que a ABIN somente poderá comunicar-se com os demais órgãos da administração pública com o conhecimento prévio da autoridade competente de maior hierarquia do respectivo órgão, ou um seu delegado (art. 10, Lei 9.883/1999).

1.4.4 Fiscalização pelo judiciário

A fiscalização pelo judiciário é a mais adequada para o controle da licitude de operações específicas de inteligência, especialmente sobre sua compatibilidade com as garantias legais de proteção aos direitos humanos. Membros do judiciário são independentes da estrutura burocrática da administração e portanto estão, ao menos em tese, aptos a oferecer uma visão externa sobre as atividades de inteligência, o que confere credibilidade ao sistema de fiscalização aos olhos do público.¹⁶⁰

Não obstante, há problemas na fiscalização pelo judiciário. Inicialmente, um procedimento judicial que escrutine atividades de inteligência implica a retirada de informação classificada de seu ambiente original de controle. Mesmo que se sujeite o procedimento ao “segredo de justiça”, os juízes, advogados e os funcionários do órgão judicial terão contato com a informação classificada. Por essa razão normalmente se estabelecem procedimentos judiciais específicos que garantam o sigilo da informação compartilhada no processo, a exemplo do que ocorre nos Estados Unidos, Canadá e Reino Unido.¹⁶¹

Há nesse processo, como aponta Ian Leigh, o risco de que juízes, ao se familiarizarem com as técnicas, fontes e operações através de um contato frequente com informações classificadas em processos judiciais, se tornem enviesados, ou “aclimatizados”, em favor dos serviços de inteligência. “Isso sugere um padrão de declínio de efetividade na proteção de direitos individuais na prática”.¹⁶² De fato, serve como exemplo desse efeito a experiência da *Foreign Intelligence Surveillance*

¹⁵⁹ *Ibidem*. p. 70.

¹⁶⁰ *Ibidem*. p. 75.

¹⁶¹ *Ibidem*. p. 75-76.

¹⁶² *Ibidem*. p. 76.

*Court (FISC)*¹⁶³, a corte secreta dos Estados Unidos que entre os anos de 1979 e 2015, de um total de 38.365 pedidos de vigilância eletrônica recebeu 38.269, dos quais apenas 12 terminaram por ser rejeitados.¹⁶⁴ (conferir no **Anexo 4** uma ordem secreta da *FISC* determinando à empresa de telecomunicações Verizon a entrega diária à *NSA* de metadados de todas ligações em que um dos interlocutores estivesse presente em território dos Estados Unidos).

1.4.5 Fiscalização por atores internacionais

Por fim, os serviços de inteligência estatal também estão sujeitos a algum grau de fiscalização externa por atores internacionais, em que se incluem Cortes e Organizações Internacionais e governos estrangeiros. O melhor exemplo do exercício de controle internacional das agências de inteligência se verifica na experiência da Corte Europeia de Direitos Humanos (CEDH) na fiscalização da proteção do direito à privacidade no exercício de atividades de vigilância nos Estados europeus. Na seção 4.3.1 (“A Proteção Internacional do Direito Humano à Privacidade”) se faz uma análise detalhada da jurisprudência da CEDH nessa tarefa. Há nessa hipótese legítima forma de controle judicial internacional dos serviços de inteligência.

A ONU recentemente demonstra crescente preocupação com a proteção internacional do direito humano à privacidade no contexto da vigilância em massa, o que se comprova na aprovações de resoluções da Assembleia Geral sobre o direito à privacidade na era digital e atividades de vigilância na tarefa de combate ao terrorismo. Além disso, recentemente se instituiu o cargo de Relator Especial Sobre

¹⁶³ A *FISC* é composta por 11 juízes publicamente indicados pelo *Chief Justice* para um mandato de 7 anos sem recondução, ao menos 3 dos quais devem residir a no máximo 20 milhas de Washington D.C., disposição que se justifica dada a urgência que a apreciação de determinados pedidos de vigilância possam exigir. A Corte possui jurisdição para emitir mandados de busca e apreensão e de vigilância eletrônica para fins de coleta de informação estrangeira (*foreign intelligence*). Apesar de existir um procedimento de publicação dos votos dos juízes da Corte, isso só ocorre em situações extremamente excepcionais, sendo o sigilo a regra. Um grupo de 3 juízes aprecia os pedidos, havendo em contrapartida a *Court of Review* com competência para rever a decisão, composta de três outros juízes. Caso um pedido das agências governamentais seja rejeitado também na *Court of Review*, ele pode ser revisto pela Suprema Corte através de uma *petition of certiorari*. Cf. CONGRESSIONAL RESEARCH SERVICE. **The U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review: An Overview**, 24 jan. 2007.

¹⁶⁴ ELETRONIC INFORMATION PRIVACY CENTER. **Foreign Intelligence Surveillance Act Court Orders – 1979-2015**. Disponível em: <<https://epic.org/privacy/surveillance/fisa/stats/default.html>>

o Direito à Privacidade, com especial atenção ao problema da coleta cibernética de informações privadas (cf. seção 4.3.1).

Pode se dizer ainda que Estados estrangeiros também exercem certo grau de fiscalização sobre serviços nacionais de inteligência, especialmente quando se trata de redes de compartilhamento de informações, cujos membros assumem o compromisso de não espionar uns aos outros. Além disso, como explica Ashley Deeks, um parceiro de uma rede de compartilhamento pode decidir internamente que não pode receber informações de outro membro que foram coletadas com violação a direitos humanos, pois isso iria infringir a sua própria legislação.¹⁶⁵ Por exemplo, o Canadá, parceiro dos Estados Unidos no grupo *Five Eyes*, poderia recusar receber informações da NSA que foram coletadas em termos que violariam a própria legislação interna. Mas é preciso que se observe, todavia, que esse tipo de fiscalização é bastante precária pois, especialmente quando se trata dos Estados Unidos, a maior parte de seus parceiros não pode se dar ao luxo de recusar o suporte de sua robusta capacidade de inteligência.¹⁶⁶

¹⁶⁵ DEEKS, Ashley. An International Legal Framework for Surveillance. **Virginia Journal of International Law**, v. 55, 2015. p. 325.

¹⁶⁶ “Most other countries cannot afford to break off intelligence cooperation with the United States because they rely on U.S. intelligence assistance to protect themselves from national security threats”. POSNER, Eric A. **Statement to the Privacy & Civil Liberties Oversight Board**, 14. mar. 2014. Disponível em: <<https://www.pclob.gov/library/20140319-Testimony-Posner.pdf>>

2 O ATUAL CONTEXTO POLÍTICO DO EXERCÍCIO DA INTELIGÊNCIA DE ESTADO – A RETÓRICA DA SEGURANÇA NA ERA DO MEDO

“Men fear death as children fear to go in the dark; and as that natural fear in children is increased with tales, so is the other”. (Francis Bacon)¹⁶⁷

*“we are judged by what we do not know and did not prevent”.*¹⁶⁸

(“Eliza” Manningham-Buller, Diretora Geral do MI5 de outubro de 2002 a abril de 2007).

2.1 O impacto político-jurídico dos ataques de 11 de setembro de 2001

O ataque terrorista de 11 de setembro de 2001 está gravado na memória das pessoas pela imagem dos dois prédios do *World Trade Center*, tido como o coração financeiro dos Estados Unidos, em chamas. A menção à fatídica data, a que a expressão “ataque às torres gêmeas” se tornou sinônima, normalmente não faz recordar a imagem do prédio do Departamento de Defesa com a porção oeste destruída. De fato, o coração militar da maior potência global, o Pentágono, um dos edifícios mais bem protegidos do mundo, também havia sofrido um duro golpe naquele dia. Um terceiro evento ocorria com a queda, no estado da Pensilvânia, de um avião que se dirigia à Washington, o coração político dos Estados Unidos, mas cujos sequestradores foram contidos pelos passageiros, já cientes de que o país estava sob ataque.

O ineditismo da ocorrência do primeiro ataque em solo continental americano em tempo de paz coordenado por um inimigo externo^{169 170}, definiu um momento de

¹⁶⁷ BACON, Francis. **Essays**, of Death. 1601.

¹⁶⁸ MANNINGHAM-BULLER, Elizabeth Lydia. **The international terrorist threat and the dilemmas in countering it**. Discurso em Ridderzaal, Binnenhof, Haia, Holanda, 2005. Disponível em: <<https://www.mi5.gov.uk/fr/node/406>>

¹⁶⁹ É importante destacar que a *al-qaeda* já anunciara claramente seus propósitos terroristas anteriormente a 2001, dando prova de sua capacidade operacional com ataques a bomba às embaixadas dos Estados Unidos em Nairóbi, no Quênia e em *Dar es Salaam*, Tanzânia, em 07 de agosto de 1998.

¹⁷⁰ Em situações de beligerância, dois episódios pouco conhecidos da Segunda Guerra Mundial merecem menção, além do bombardeamento de Pearl Harbor. Em primeiro lugar um ataque de um submarino japonês a um depósito militar em Fort Stevens, Oregon, no estuário do Rio Columbia, na costa oeste dos EUA. Foi o primeiro ataque de uma potência estrangeira no território continental americano desde os ataques da guerra de 1812, mas os danos foram de pequena monta. Cf. GILBERT, M. *op. cit.* p. 422. O outro evento trata-se da empreitada militar japonesa no final da guerra consistente no lançamento de balões de hidrogênio de grande altitude, armados com bombas incendiárias, que atingiram alguns pontos da costa oeste dos Estados Unidos, vindo

ruptura histórica que provocou significativas mudanças em todas as esferas da sociedade estadunidense. Da política externa à cultura, o sentimento de que o país estava diante de um poderoso inimigo, capaz de lhe infligir danos catastróficos e sem precedentes, moldou toda a retórica estatal norte-americana da primeira década do século XXI e com ela o imaginário coletivo. Com massivo apoio da opinião pública interna, o governo republicano de George W. Bush deflagrou duas grandes empreitadas militares sob a bandeira da “Guerra ao Terror”: a invasão do Afeganistão e do Iraque – muito embora o último não tivesse qualquer relação com os ataques terroristas de 11 de setembro de 2001.¹⁷¹

A ideia da guerra ao terror, como afirma David Holloway, “era por si só uma representação de eventos, uma construção retórica, uma série de histórias sobre o onze de setembro e sobre o lugar dos Estados Unidos no mundo”.¹⁷² A derrubada das torres gêmeas logo se converteu em um símbolo de ataque ao mundo livre, à democracia, e ao capitalismo e seus responsáveis em um inimigo comum do povo americano. E, superada a ameaça soviética e a guerra do golfo, já não havia quem servisse a esse papel, o de inimigo, há dez anos.

O ambiente de medo generalizado gerado pelos ataques favoreceu a aprovação e implementação de um grande número de leis – e outras medidas menos legítimas – relativas à segurança e defesa, especialmente ligadas à aviação civil, atividades militares, persecução penal e principalmente inteligência – reflexos

a provocar a morte de cinco crianças e uma mulher grávida também no estado do Oregon. A cobertura dos eventos foi censurada na imprensa para evitar que os japoneses acreditassem ter tido sucesso com os ataques e continuassem o envio dos balões. De fato, os ataques se revelaram um fiasco do ponto de vista estratégico, sendo brevemente encerrados pelo Japão. Cf. COEN, Ross. **FU-GO: The Curious History of Japan’s Balloon Bomb Attack on America**. University of Nebraska Press, 2014.

¹⁷¹ A inteligência dos Estados Unidos foi constantemente pressionada a encontrar qualquer indício que pudesse estabelecer um vínculo entre Saddam Hussein e Bin Ladin. Nos termos colocados por Paul Pillar: “*The reason the connection got so much attention was that the administration wanted to hitch the Iraqi expedition to the ‘war on terror’ and the threat the American public feared most, thereby capitalizing on the country’s militant post-9/11 mood*”. PILLAR, *op. cit.* p. 20. O Presidente Bush chegara a afirmar publicamente em setembro de 2002 que “Não se pode distinguir entre a *al-qaeda* e Saddam quando se fala em guerra ao terror”. DROGIN, B. *op. cit.* p. 126. O esforço do governo norte-americano em tentar vincular os ataques a Saddam Hussein – posteriormente convertido em uma tentativa de provar que o Iraque detinha armas de destruição em massa – surtiu efeitos. Em agosto de 2003, pesquisas de opinião pública demonstraram que 69% dos norte-americanos acreditavam que o ditador iraquiano teve envolvimento com os ataques de 11 de setembro de 2001. Cf. KORNBLUT, Anne E. and BENDER, Bryan. Cheney link of Iraq, 9/11 challenged. **The Boston Globe**, 16 ago. 2003. Disponível em: <http://www.boston.com/news/nation/articles/2003/09/16/cheney_link_of_iraq_911_challenged>

¹⁷² HOLLOWAY, David. **9/11 and the War on Terror**, Edinburgh University Press, 2008. p. 4. “*The idea of a war on terror was itself a representation of events, a rhetorical construction, a series of stories about 9/11 and about America’s place in the world*”.

percebidos não somente nos EUA mas também em aliados mais próximos, notadamente o Reino Unido.¹⁷³

No mesmo mês de setembro o presidente Bush assina ordens executivas secretas autorizando a ampliação dos poderes da CIA, principalmente para a condução de operações encobertas em território estrangeiro. Inclui-se nisso a concessão de US\$ 800 a 900 milhões para a construção de centros de inteligência contraterrorista em outros países.¹⁷⁴ Em outubro, outra dessas ordens secretas autorizou que a NSA efetuasse escutas sobre comunicações de cidadãos estadunidenses, sem a necessidade de autorização judicial como determinava a legislação.^{175 176} O próprio presidente Bush afirmou posteriormente ter renovado essa ordem por mais de 30 vezes.¹⁷⁷ A conveniência prática motivou a medida. Como explica Ron Suskind, seria um desafio logístico para a administração ter que obter mandados judiciais de escutas de milhares de cidadãos norte-americanos vigiados pelo “olho cego dos insones computadores da NSA”.¹⁷⁸

Mas a principal reação jurídico-política pós atentados terroristas de 11 de setembro de 2001 foi a aprovação, também em outubro, do USA PATRIOT ACT (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*).¹⁷⁹ O ato ampliou extensamente os poderes de investigação de agências responsáveis pelo *law enforcement* nos Estados Unidos, a que correspondeu o mínimo de controle judicial. Nesse propósito, as agências responsáveis pela inteligência externa norte-americana foram especialmente agraciadas através da seção 215 do ato, que promoveu emendas ao *Foreign Intelligence Surveillance Act (FISA)*. No ano seguinte, em setembro de 2002, a administração Bush aprova o *National Security Strategy* com demonstrações claras

¹⁷³ Cf. MORAN, Jon; PHYTHIAN, Mark. **Intelligence, Security and Policing Post-9/11: The UK's Response to the 'War on Terror'**. Palgrave Macmillan, 2008.

¹⁷⁴ SUSKIND, Ron. **The One Percent Doctrine**. Simon & Schuster, 2006. p. 22.

¹⁷⁵ RISEN, James; LICHTBLAU, Eric. Bush Lets U.S. Spy on Callers Without Courts. **The New York Times**, 16 dez. 2015. Disponível em: <http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0>

¹⁷⁶ KITROSSER, Heidi. Macro-Transparency” as Structural Directive: A Look at the NSA Surveillance Controversy. **Minnesota Law Review**, v. 91, pp. 1163-1208, 2007.

¹⁷⁷ BUSH says he signed NSA wiretap order. **CNN International**, 18 dez. 2015. Disponível em: <<http://edition.cnn.com/2005/POLITICS/12/17/bush.nsa/>>

¹⁷⁸ SUSKIND, R. *op. cit.* p. 36.

¹⁷⁹ O texto integral do PATRIOT ACT pode ser lido em: UNITED STATES CONGRESS. Congress.gov. H.R. 3162 - USA PATRIOT ACT. <<https://www.congress.gov/bill/107th-congress/house-bill/3162/text>>

da doutrina da guerra preventiva¹⁸⁰, em que atividades de inteligência iriam realizar um papel central.

O exemplo dos Estados Unidos é, certamente, o mais dramático em razão da extensão dos ataques de 11 de setembro de 2001 e da distinta capacidade do país de responder militar e politicamente a estes eventos, seja com reformas internas que ampliem poderes de inteligência, seja exercendo pressão sobre outros Estados para que conformem com seu modelo de combate ao terrorismo. Mas a era do medo havia apenas começado naquele ano, seja para os países ocidentais, alguns dos quais viriam a ter que lidar com outros ataques terroristas e, é preciso que se reconheça, também em Estados islâmicos do oriente, onde a bandeira da guerra ao terror iria cobrir grandes campanhas militares por períodos que excederam à Segunda Guerra Mundial.

Assim, países aliados aos Estados Unidos que posteriormente se viram alvos de ataques terroristas, experimentaram um impacto de mesma natureza, ainda que em menor intensidade. Em 11 de março de 2004, militantes de uma célula terrorista islâmica posicionada em Madrid detonaram, em um ataque coordenado, 10 bombas em quatro trens de passageiros, causando a morte de 191 pessoas e ferimentos em 2.050.¹⁸¹ O evento, que ficou conhecido como “11-M”, foi o pior ataque terrorista da Europa desde a queda, também em virtude da explosão de uma bomba, do avião da Pan Am que fazia o voo 103, em Lockerbie, Escócia, quando morreram 270 pessoas. Revelou-se posteriormente que a motivação dos ataques em Madrid foi o fato de a Espanha estar diretamente envolvida na Guerra do Iraque.

Além da retirada das tropas espanholas do solo iraquiano, as principais reformas no aparato de segurança do Estado conduzidas pelo novo governo espanhol, eleito três dias após os ataques, foi a criação do *Centro Nacional de*

¹⁸⁰ Em trechos tais como: “[...] *defending the United States, the American people, and our interests at home and abroad by identifying and destroying the threat before it reaches our border*” e “*While we recognize that our best defense is a good offense, we are also strengthening America’s homeland security to protect against and deter attack*”. Cf. UNITED STATES OF AMERICA. **The National Security Strategy of the United States of America**, The White House, 2002. p. 6. Disponível em: <<http://www.state.gov/documents/organization/63562.pdf>>

¹⁸¹ Provou-se que os ataques foram orquestrados por militantes islâmicos mas nunca foi possível estabelecer com certeza qualquer vínculo dos autores com a *al-qaeda*. Qualquer suspeita de que os separatistas bascos do *Euskadi Ta Askatasuna* (ETA) possam ter sido responsáveis pelas explosões foi oficialmente descartada. Cf. ADMINISTRACIÓN DE JUSTICIA. **Juzgado Central de Instrucción nº 6**, 10 abr. 2006. p. 1412. Disponível em: <<http://www.elmundo.es/documentos/2006/04/11/autohtml/index.html?cual=1412>> e HAMILOS, Paul; TRAN, Mark. 21 guilty, seven cleared over Madrid train bombings, **The Guardian**, 31. Out. 2007. Disponível em: <<http://www.theguardian.com/world/2007/oct/31/spain.marktran>>

Coordinación Antiterrorista (CNCA) que exerce importante papel na integração da inteligência do país além do já existente *Centro Nacional de Inteligencia*; o estabelecimento de um plano abrangente de combate ao terrorismo (*Plan Operativo de Lucha Contra el Terrorismo*); e a criação de novas unidades na divisão de contraterrorismo da Polícia Nacional, a *Comisaría General de Información*, em áreas de análise estratégica, sistemas e tecnologias de informação e terrorismo cibernético.¹⁸²

No ano seguinte, em 7 de julho de 2005, um dia após ter sido anunciada como sede dos Jogos Olímpicos de 2012, Londres também foi alvo de ataques terroristas de extremistas islâmicos. Quatro bombas foram detonadas – 3 no sistema metroviário, o *London Underground*, e outra em um dos famosos ônibus vermelhos *double-decker* – causando a morte de 52 pessoas e ferimentos em mais de 500. Tal como em Madrid, a motivação dos ataques foi o envolvimento britânico com a Guerra do Iraque.

O 7/7 londrino resultou na conclusão oficial de que o ataque não poderia ter sido evitado ou antecipado com as informações que a inteligência detinha ao momento, diferentemente do que se diz em relação ao 9/11.^{183 184} De qualquer forma, a inteligência britânica foi alvo de significativas reformas, a começar pelo orçamento do *MI5* – a agência de segurança e contraterrorismo do país – que triplicou após 2005.¹⁸⁵ Outras agências de inteligência, em especial o *MI6* e o *GCHQ*, tiveram potencializada sua capacidade de inteligência externa, com especial atenção à identificação de campos de treinamento terrorista, incluindo acordos de cooperação com autoridades paquistanesas. Reforçando tal política, o *Terrorism Act* de 2006 define como crime a presença de cidadãos britânicos em locais dedicados ao treinamento terrorista, seja dentro ou fora do Reino Unido (Part I, 8). O ato também promoveu emendas ao *Intelligence Services Act* de 1994 e à *The*

¹⁸² REINARES, Fernando. After the Madrid Bombings: Internal Security Reforms and the Prevention of Global Terrorism in Spain. *Studies in Conflict & Terrorism*, v. 32, n. 5, 2009.

¹⁸³ INTELLIGENCE AND SECURITY COMMITTEE. **Could 7/7 Have Been Prevented?** Review of the Intelligence on the London Terrorist Attacks on 7 July 2005, mai. 2009.

¹⁸⁴ Todavia, a notícia de que o *MI5* havia reaberto uma investigação anterior sobre dois dos responsáveis pelos ataques, que foi acompanhada pela saída precoce da Diretora Geral do *MI5*, Eliza Manningham-Buller, em abril de 2007, é vista por alguns comentaristas como um sinal de admissão da falha da agência em compartilhar todas as informações com o *Intelligence and Security Committee*, órgão ao qual foi incumbida a tarefa de analisar a atuação das agências de segurança e possíveis falhas de inteligência no 7/7. (nota supra) Cf. PHYTHIAN, Mark. In the Shadow of 9/11: Security, Intelligence and Terrorism in the United Kingdom. In: MORAN, J.; PHYTHIAN, M. *op. cit.* p. 36.

¹⁸⁵ *Ibidem.* p. 45.

Regulation of Investigatory Powers Act de 2000, ampliando poderes de vigilância de agências de investigação.¹⁸⁶ Destaca-se aqui a crescente cooperação do *GCHQ* com a *NSA* e outras agências do consórcio *Five Eyes* na condução da inteligência de sinais, como ficou exposto nos documentos vazados por Edward Snowden.¹⁸⁷

Além de Estados Unidos e Europa, o caso de Israel oferece um exemplo valioso pois a estratégia de sua inteligência está ligada a um contexto mais amplo se comparada com a de seus aliados ocidentais. O exercício da inteligência em Israel está intimamente associado à contínua rivalidade com países vizinhos árabes e com o povo palestino. Sem buscar estabelecer aqui qualquer juízo de valor sobre os conflitos, pode-se afirmar que Israel convive com ataques terroristas, tal como sua percepção, muito antes do surgimento das atuais alas radicais do islamismo e sua oposição aos Estados Unidos e aliados, movimento esse que encontra suas raízes no fim da guerra fria (*al-qaeda*) e na desastrosa invasão do Iraque em 2003 (*ISIS*).¹⁸⁸

Até a intensificação do conflito com o *Hamas* no ano de 2001, a estratégia da inteligência e da política externa israelense focava-se em quatro principais questões: a possibilidade de guerra contra a Síria; o fortalecimento do *Hezbollah* no Líbano; a possibilidade de implementar um acordo de *status* permanente com os palestinos e o programa de desenvolvimento de mísseis de longo alcance do Irã.¹⁸⁹ O discurso instalado após o 11/9 de que havia uma “insurgência global” do terrorismo islâmico contra o mundo ocidental¹⁹⁰ facilitou os esforços coordenados da “guerra contra o

¹⁸⁶ UNITED KINGDOM. **Terrorism Act**, 2006.

¹⁸⁷ Conferir por exemplo: HOPKINS, Nick. UK gathering secret intelligence via covert NSA operation. **The Guardian**, 7 jun. 2013. Disponível em: <<http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism>>

¹⁸⁸ Apesar de os Estados Unidos terem financiado e apoiado operacionalmente grupos de resistência à invasão soviética no Afeganistão, os chamados *mujahedin*, inclusive com operações encobertas da *CIA*, não há evidências de que tenha havido um financiamento direto a Bin Ladin ou que de outra forma se tenha contribuído para a formação da *al-qaeda*. Ocorre que, ao fim da guerra fria, há um ressentimento com a presença militar dos Estados Unidos na Arábia Saudita e com o apoio do país a Israel, razões centrais dos ataques terroristas nos anos que se seguiram. Já o chamado “Estado Islâmico” é fruto de um movimento de proliferação de células terroristas no Iraque após a guerra de 2003 que ganha força com a guerra civil da Síria a partir de 2011. Cf. UNITED STATES OF AMERICA. **The 9/11 Commission...** *op. cit.* p. 408-410; BYMAN, Daniel. **Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs to Know**. Oxford University Press, 2015 p. 3-6 e 164-167.

¹⁸⁹ KUPERWASSER, Yosef. **Lessons from Israel's Intelligence reforms**, analysis paper, n. 14. The Saban Center at The Brookings Institution, 2007.

¹⁹⁰ Uma crítica incisiva à ideia de “insurgência global” do islamismo é feita por Sherifa Zuhur: “[...] *the so-called “global insurgency,” is not singular, has no sole center of gravity, and advised narrowing the field of enemies to those “militant” Islamists who are also violent and coercive, not those who pose no reasonable threat to the United States. It is not in the name of political correctness and tolerance that we should be aware of the overlap between potentially violent radicals and nonthreatening figures, it is because the effort to pursue “militant Islam” instead of simply opposing*

terror”, e ajudou a intensificar sensivelmente o apoio do governo americano a Israel durante a gestão republicana, fortalecendo sua estratégia de contenção da população palestina e de estados rivais árabes vizinhos. Após o conflito com o *Hezbollah* em 2006, e o enfraquecimento da Síria, as principais questões de segurança de Israel atualmente são o conflito interno com os palestinos e a possibilidade de um confronto bélico de maiores proporções com o Irã a longo prazo¹⁹¹, apesar de que as mudanças de regime decorrentes da chamada “primavera árabe” alçaram ao poder governos islâmicos não simpáticos a Israel no Egito, Marrocos e Kuwait.¹⁹²

Esse cenário se refletiu, em relação aos palestinos, numa postura mais agressiva do *Shin Bet* (ou *Shabak*), a agência de segurança de Israel, responsável pela inteligência interna do país – incluindo-se aqui os territórios ocupados. Já no que toca à política externa israelense, cujo foco é frear as ambições nucleares do Irã, vistas como a maior ameaça ao Estado de Israel, a situação é mais delicada pois envolve risco de escalada militar a nível regional caso se agravem as relações entre os dois países. Meir Dagan, ex-chefe do *Mossad*, a agência de inteligência externa israelense, declarado opositor das políticas do primeiro-ministro Benjamin Netanyahu, afirmou que qualquer ação militar contra o Irã resultaria em um conflito regional que ameaçaria a existência do Estado de Israel.¹⁹³ Considerando ainda que o Irã possui o maior inventário de mísseis balísticos do Oriente Médio¹⁹⁴, um ataque militar direto ao país parece ser uma opção viável apenas em casos extremos, portanto.

Dessa forma, a política de contenção do programa nuclear iraniano exigiu especial esforço da inteligência em atividades de espionagem e operações

“terrorism,” is too grand a project — one that points at all those who oppose U.S. policies, and even some of our allies who do not”. ZUHUR, Sherifa. **Precision in the Global War on Terror**: Inciting Muslims through the War of Ideas. Strategic Studies Institute, 2008. p. 9.

¹⁹¹ A *al-qaeda*, que até o momento não realizou nenhum ataque em território israelense, não é apontada pelos analistas de política externa como uma ameaça imediata a Israel. Uma possível explicação é a presença do *Hamas* e do *Hezbollah* nas fronteiras do país, organizações que são hostis a *al-qaeda*. BYMAN, D. *op. cit.* p. 134.

¹⁹² VOLLER, Yaniv. After the Arab Spring: power shift in the Middle East?: turmoil and uncertainty: Israel and the New Middle East. **IDEAS Reports**, London School of Economics, 2012.

¹⁹³ URQUHART, Conal. Israel government 'reckless and irresponsible' says ex-Mossad chief. **The Guardian**, 3 jun. 2011. Disponível em: <<http://www.theguardian.com/world/2011/jun/03/israel-government-reckless-mossad-chief>>

¹⁹⁴ OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. **Worldwide Threat Assessment of the US Intelligence Community**, 26 fev. 2015. p. 6.

encobertas, fato reconhecido por Meir Dagan.¹⁹⁵ Nisso se incluem operações de ataque cibernético a sistemas de usinas de enriquecimento de urânio do Irã, conduzidas em conjunto com os Estados Unidos¹⁹⁶ e, especula-se, assassinatos de físicos iranianos em ações encobertas do *Mossad*.¹⁹⁷

Recentemente, tal política foi desafiada pelas negociações dos chamados P5+1 (Os cinco membros com representação permanente no Conselho de Segurança da ONU, EUA, Reino Unido, França, China, Rússia e, adicionalmente, a Alemanha) com o Irã, que resultaram em um acordo de limitação de sua capacidade de enriquecimento de urânio, o chamado *Joint Comprehensive Plan of Action*, sob rigorosa fiscalização da Agência Internacional de Energia Atômica (AIEA) (cf. seção 6.4.1). O governo Netanyahu se opõe vigorosamente ao acordo¹⁹⁸ e há indícios de que a inteligência israelense espionou as negociações – inclusive o então secretário de Estado americano John Kerry – para fornecer informações à oposição republicana nos Estados Unidos, tentando minar a ratificação.^{199 200 201}

¹⁹⁵ Como reconhecido pelo ex-chefe do *Mossad*, em entrevista ao jornal israelense *Ynetnews*, quando questionado se houveram operações clandestinas contra o Irã: "There were. We always said that the Iranian nuclear program could be delayed but that it was impossible to destroy it by means of clandestine operations". BARNEA, Nahum; SHIFFER, Shimon. "Netanyahu has caused Israel the most strategic damage on Iran". **Ynetnews.com**, 27 fev. 2015. Disponível em: <<http://www.ynetnews.com/articles/0,7340,L-4631634,00.html>>

¹⁹⁶ O ataque consistiu no desenvolvimento de um sofisticado vírus de computador, hoje conhecido como *stuxnet*, capaz de proporcionar ao seus operadores o controle de equipamentos de plantas industriais. Estima-se que o ataque tenha sido capaz de retirar de operação cerca de mil das cinco mil centrífugas que o Irã possuía ao momento. Cf. SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. **The New York Times**, 1 jun. 2012. Disponível em: <<http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=4&r=1&hp>>; KELLEY, Michael B. The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. **Business Insider**, 20 nov. 2013. Disponível em: <<http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11>>; NORTON. **The Stuxnet Worm**. Disponível em: <<http://us.norton.com/stuxnet>>

¹⁹⁷ FITSANAKIS, Joseph. "We killed Iranian scientist" claims Israel intel source. **Intelnews.org**, 03 ago. 2011. Disponível em: <<http://intelnews.org/2011/08/03/01-778/>>; RAVIV, Dan. U.S. pushing Israel to stop assassinating Iranian nuclear scientists. **CBS News**, 1 mar. 2014. Disponível em: <<http://www.cbsnews.com/news/us-pushing-israel-to-stop-assassinating-iranian-nuclear-scientists/>>

¹⁹⁸ O primeiro-ministro israelense chegou a discursar no Congresso norte-americano em 2015, sem ter sido convidado pela Casa Branca, quando apresentou suas razões de contrariedade ao acordo nuclear. O discurso pode ser assistido em BENJAMIN Netanyahu Speech to Congress 2015. **The New York Times**, Disponível em: <<https://www.youtube.com/watch?v=wRf1cdw4IAY>>

¹⁹⁹ ENTOUS, Adam. Israel Spied on Iran Nuclear Talks With U.S. **The Washington Post**, 23 mar. 2015. Disponível em: <<http://www.wsj.com/articles/israel-spied-on-iran-talks-1427164201>> Acesso em: _____; WIRETAPPED: Israel Eavesdropped on John Kerry in Mideast Talks. **Der Spiegel Online**, 03 ago. 2014. Disponível em: <<http://www.spiegel.de/international/world/israel-intelligence-eavesdropped-on-phone-calls-by-john-kerry-a-984246.html>>

²⁰⁰ Apesar de aliados e de compartilharem informações com propósitos contraterroristas, documentos classificados vazados da NSA demonstram que há um longo histórico de espionagem entre Estados Unidos e Israel. GREENWALD, Glenn; FISHMAN, Andrew. Netanyahu's Spying Denials

2.2 Percepção de ataques terroristas como resultado de falhas de inteligência

Decididos a avaliar como um ataque de tamanha proporção se fez possível, mesmo com todo o aparato de defesa e inteligência dos Estados Unidos, foi formada uma comissão bipartidária – composta por cinco congressistas republicanos e cinco democratas – instaurada com a responsabilidade de atingir a “maior compreensão possível dos eventos relacionados ao onze de setembro e identificar as lições aprendidas”. Foi averiguado que as agências de inteligência do país, especialmente a *CIA* e o *FBI*, falharam em associar as poucas informações que tinham a respeito dos terroristas presentes em solo americano e ignoraram alertas importantes sobre a possível iminência de um ataque coordenado pela *al-qaeda*.

Um dos mais importantes alertas nesse sentido ficou conhecido como “*Phoenix Memo*”, um relatório de um oficial do *FBI* posicionado na capital do Arizona dirigido à sede e à divisão de combate ao terrorismo da agência, informando sobre um número excessivo de indivíduos de “interesse investigativo” frequentando aulas de pilotagem no estado. O próprio oficial conclui no relatório que tal circunstância provavelmente era resultado de “esforços coordenados de Usama Bin Ladin”.²⁰²

Em Minneapolis, agentes do *FBI* também identificaram um indivíduo que frequentava cursos de pilotagem e nutria crenças *jihadistas*, sendo descrito como “um extremista islâmico se preparando para um ato futuro em apoio a objetivos radicais fundamentalistas”.²⁰³ Esse indivíduo, como cidadão francês, foi preso por ter excedido seu tempo de estadia nos Estados Unidos mas não foi investigado profundamente, não obstante as evidências de ligações terroristas, em razão de restrições legais de disposições do *FISA* até então vigentes. Tratava-se de Zacarias Moussaoui um membro da *al-qaeda* com envolvimento direto com os terroristas responsáveis pelo sequestro dos aviões.²⁰⁴

Contradicted by Secret NSA Documents. **The Intercept**, 25 mar. 2015. Disponível em: <<https://theintercept.com/2015/03/25/netanyahus-spying-denial-directly-contradicted-secret-nsa-documents/>>

²⁰¹ Apesar dos esforços republicanos, o acordo foi ratificado no Congresso dos Estados Unidos, mas ainda encontra resistência na implementação de seus termos.

²⁰² UNITED STATES OF AMERICA. **The 9/11 Commission Report**, National Commission on Terrorists Attacks Upon the United States, 2004. p. 272.

²⁰³ “an Islamic extremist preparing for some future act in furtherance of radical fundamentalist goals”. *Ibidem*, p. 273.

²⁰⁴ *Ibidem*, p. 274-276.

Não bastasse, nas 72 horas que antecederam os ataques, a NSA Interceptou quatro comunicações sugerindo que um ataque terrorista era iminente. Em um dos trechos mais significantes, um dos interlocutores diz “O grande jogo está para começar”. Em outro se pode ouvir: “amanhã é a hora zero”. Todavia, a agência não traduziu e disseminou a informação até o dia 12 de setembro.²⁰⁵

Acresça-se a isto o fato de ter sido o presidente Bush informado pessoalmente, no *President's Daily Brief* de 6 de agosto de 2001, intitulado “*Bin Ladin determined to attack in U.S.*” (conferir **Anexo 2**) de que:

Membros da Al-Qa'ida – incluindo alguns que são cidadãos dos Estados Unidos – tem residido ou viajado para os Estados Unidos por anos, e o grupo aparentemente mantém uma estrutura de apoio que pode auxiliar em ataques. [...] Nós não fomos capazes de corroborar alguns dos relatórios de ameaças mais extraordinários, tais como o do serviço [parte não desclassificada] de 1998 dizendo que Bin Ladin queria sequestrar um avião americano para obter a soltura do “Cheique Cego” Umar Abd al-Rahman e outros prisioneiros extremistas. Não obstante, informações do FBI desde o momento indicam padrões de atividades suspeitas no país consistentes com preparações para sequestros e outros tipos de ataques, incluindo vigilância recente sobre prédios federais em Nova York.²⁰⁶

Esse foi o trigésimo sexto *Daily Brief* que o Presidente Bush recebera em 2001 relatando atividades de Bin Ladin ou da *al-qaeda*.²⁰⁷

Diante de tais informações, as conclusões alcançadas pela “Comissão 11/9”, expostas em um relatório de 567 páginas, consistiram no alerta da premente necessidade de reformular a comunidade de inteligência norte-americana, diante de seis problemas fundamentais identificados, a saber: a) barreiras estruturais para a realização de atividades conjuntas entre agências de inteligência; b) ausência de padrões e práticas comuns entre a comunidade de inteligência doméstica e externa; c) gestão compartimentada das capacidades da inteligência nacional entre várias

²⁰⁵ AID, Matthew. **The Secret Sentry**: the untold history of the national security agency. Bloomsbury Press, 2009. p. 243.

²⁰⁶ “Al-Qa'ida members – including some who are U.S. citizens – have resided in or traveled to the US for years, and the group apparently maintains a support structure that could aid attacks [...] We have not been able to corroborate some of the more sensational threat reporting, such as that from a ----- service in 1998 saying that Bin Ladin wanted to hijack a US aircraft to gain the release of “Blind Shaykh” Umar ‘Abd al-Rahman and other US-held extremists. Nevertheless, FBI information since that time indicates patterns of suspicious activity in this country consistent with preparations for hijackings or other types of attacks, including recent surveillance of federal buildings in New York”. BIN Ladin determined to strike in US. president's daily brief, 6 ago. 2001.

²⁰⁷ GILL, P. op. cit. In: JOHNSON, L. K. **Strategic...**, v.1., op. cit. p. 160.

agências; d) fraca capacidade de estabelecer prioridades e distribuir recursos; e) existência de cargos com acúmulo de atribuições e f) a excessiva complexidade e segredo que obscureciam o serviço de inteligência para o público.²⁰⁸

Formou-se portanto uma crença de que a inteligência dos Estados Unidos falhara decisivamente para que os ataques terroristas viessem a ter êxito; a correção dessas falhas, concluiu-se, poderia evitar a ocorrência de novos ataques e com isso resultar na preservação da vida de centenas de cidadãos estadunidenses.

Tudo isso serviu de justificativa à implementação de sensíveis reformas na inteligência do país, o que normalmente significou ampliação de seus poderes. Aproximadamente cinco meses após a publicação do relatório da “Comissão 11/9”, o Presidente G. W. Bush assina o *Intelligence Reform and Terrorism Prevention Act*, promovendo substanciais mudanças estruturais na organização da comunidade de inteligência dos Estados Unidos²⁰⁹, notadamente a criação do cargo-chefe de Diretor Nacional de Inteligência. (cf. seção 1.3, item i).

Em 2007 e 2008, ainda sob a administração Bush, ocorrem as mais agressivas modificações na inteligência dos EUA, através da aprovação de novas emendas ao *Foreign Intelligence Surveillance Act*. Tais reformas virtualmente eliminaram a necessidade de obtenção de autorização judicial para condução de atividades de vigilância, inclusive sobre comunicações de cidadãos de outros países. Além disso, previam imunidade de jurisdição para companhias privadas de comunicação que colaborassem com agências de inteligência na coleta de informação.^{210 211} Isso permitiu o desenvolvimento dos mais intrusivos programas de espionagem por parte da NSA e outras agências de inteligência aliadas, incluindo-se o PRISM – brevemente descrito na seção 1.2.2, b (Inteligência de sinais) – que começou a ser operado em 2007.

A partir de 2013 pode-se identificar uma nova manifestação extremista islâmica após o rompimento de Abu Bakr al-Baghdadi com a *al-qaeda*, e sua auto-proclamação como líder supremo do que passou então a ser conhecido como “Estado Islâmico” (do Iraque e da Grande Síria – al-Dawla al-Eslamiyya al-Iraq al-

²⁰⁸ UNITED STATES OF AMERICA. **The 9/11 Commission...** *op. cit.* p. 408-410.

²⁰⁹ O'CONNELL, Anne Joseph. The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World. **California Law Review**, v. 94, p. 1655-1744, 2006.

²¹⁰ UNITED STATES OF AMERICA. **Protect America Act**, 2007.

²¹¹ UNITED STATES OF AMERICA. **FISA Amendments Act**, 2008.

Sham – “Daesh”, ou em inglês *Islamic State of Iraq and Syria – ISIS*).²¹² De inspiração *wahabbita*²¹³, o grupo prega crenças e emprega técnicas consideradas excessivamente radicais até mesmo para outros extremistas muçulmanos.

A rivalidade que se estabelece entre estes dois grupos a partir de 2015 envolve a França como o alvo prioritário de ataques. Em 07 de janeiro de 2015 o jornal *Charlie Hebdo* sediado em Paris foi invadido por dois atiradores da *al-qaeda* que provocaram a morte de 8 funcionários, 2 policiais e 2 civis, e ferimentos em mais 12 pessoas. O ataque foi motivado por publicações do jornal que continham caricaturas de cunho satírico representando o profeta Maomé e outros líderes islâmicos. No mesmo dia, um civil e uma policial também foram alvejados por disparos de arma de fogo em outros pontos da cidade e, em 09 de janeiro, outro evento envolvendo reféns na região de *Porte de Vincennes*, leste de Paris, provocaram a morte de 4 deles.

No mesmo ano, em 13 de novembro, mesmo sob alerta máximo de terrorismo declarado pelo governo francês, Paris é novamente alvo de ataques terroristas coordenados. 130 pessoas foram mortas e 368 feridas na região de *Saint-Denis*, como resultado de explosões de homens-bombas nas proximidades do *Stade de France* e de ataques com rifles de assalto e granadas de mão em bares e restaurantes da cidade, principalmente no famoso teatro “*Bataclan*” onde 89 pessoas foram vitimadas. Os atos terroristas, reivindicados pelo “Estado Islâmico” foram motivados pelo envolvimento da França nos ataques aéreos contra alvos do grupo terrorista no Iraque e na Síria.

Como reação, o governo de François Hollande decretou situação de estado de emergência por uma semana, posteriormente prorrogado por 3 meses, que conferiu poderes de busca à polícia em qualquer residência sem necessidade de mandado judicial – com exceção de casas e escritórios de parlamentares, jornalistas e advogados. A medida também autorizava que pessoas suspeitas de representar risco à segurança nacional fossem mantidas em casa, inclusive através de

²¹² BYMAN, D. *op. cit.* p. 164.

²¹³ O *wahabbismo* é um movimento radical islâmico inspirado nos ensinamentos de Muhammad Ibn Abd al-Wahhab, particularmente influente na Arábia Saudita onde seus sectários são fortes aliados do regime sunita. O grupo adota uma forma de interpretação restrita e puritana do Corão, o que o torna hostil mesmo a outros islâmicos que praticam concepções mais moderadas, especialmente xiitas. *Ibidem.* p. 70.

monitoração eletrônica, pelo prazo de 12 horas por dia, também sem que fosse necessário para tanto um mandado judicial.²¹⁴

Antes de discutir sobre possíveis falhas na inteligência francesa, vale observar que ao momento dos ataques havia cerca de 11.000 indivíduos qualificados pelos órgãos de segurança como radicais residindo em território francês, dos quais 1.200 podiam ser considerados “combatentes” a serviço de um grupo terrorista estrangeiro.²¹⁵ Considerando que para a vigilância ininterrupta de um suspeito um aparato de segurança de 15 a 20 pessoas é necessário, a França iria precisar de cerca de 220.000 oficiais para monitorar todos eles, o que ao momento não se mostrava factível se considerarmos que o país dispunha de apenas 3.300 oficiais de inteligência disponíveis.²¹⁶

Não obstante, alguns indícios sugerem a existência de falhas graves, relacionadas aos próprios procedimentos de vigilância e à priorização na contenção de ameaças. Um inquérito parlamentar instaurado para investigar os eventos identificou múltiplas falhas nas operações de inteligência, principalmente relacionadas à problemas de comunicação com as agências de segurança sobre informações de suspeitos e indivíduos sob vigilância.²¹⁷ Descobriu-se que a inteligência francesa já conhecia ao menos 3 dos suspeitos de envolvimento nos ataques: Abelhamid Abaaoud tido como cúmplice de dois *jihadistas* mortos na Bélgica em janeiro de 2015; Omar Ismaïl Mostefai que já estava nos registros da polícia mesmo antes de ter viajado para a Síria em 2013 – o que foi alertado pela inteligência da Turquia por duas vezes²¹⁸ – e Sami Amimour que foi preso em 2012 suspeito de ligações com terroristas tendo também viajado para a Síria em 2013 e retornado para a França mesmo com um mandado de prisão internacional em aberto. Em outro episódio, Salah Abdeslam, quem alugou um dos carros utilizados

²¹⁴ GRIFFIN, Andrew. France state of emergency declared for three months, allowing authorities to shut down websites and giving police sweeping new powers. **The Independent**, 19 nov. 2015. Disponível em: <<http://www.independent.co.uk/news/world/europe/france-state-of-emergency-declared-for-three-months-allowing-authorities-to-shut-down-websites-and-a6740886.html>>

²¹⁵ CAMILLI, Edoardo. The Paris attacks. A case of intelligence failure? **NATO Review Magazine**, 2015. Disponível em: <<http://www.nato.int/DOCU/review/2015/ISIL/Paris-attacks-terrorism-intelligence-ISIS/EN/index.htm>>

²¹⁶ *Ibidem*.

²¹⁷ O texto integral do inquérito pode ser lido em: PIETRASANTA, Sébastien M. Rapport Fait au Nom de la Commission D'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015. **Assemblée Nationale**, 5 jul. 2016. Disponível em: <<http://www.assemblee-nationale.fr/14/pdf/rap-eng/r3922-t1.pdf>>

²¹⁸ YEGINSU, Ceylan. Paris Attacks: The Violence, its Victims and How the Investigation Unfolded. **The New York Times**, 16 nov. 2015. Disponível em: <<http://www.nytimes.com/live/paris-attacks-live-updates/turkey-warned-french-twice-about-attacker-official-says/>>

pelos terroristas e era irmão de um dos homens-bomba que se explodiu nas proximidades do *Comptoir Coltaire Cafe*, foi parado pela polícia na fronteira com a Bélgica poucas horas antes do ataque e foi liberado após ser questionado.²¹⁹

A ligação dos responsáveis pelos ataques em Paris com a Bélgica se tornaria clara em março de 2016 quando dois ataques à bomba coordenados no aeroporto de Bruxelas e na estação metroviária Malbeek causaram a morte de 35 pessoas, incluindo 3 “homens-bomba”, e ferimentos em mais de 300. O evento de 22 de março de 2016 ocorreu três dias após a prisão de Salah Abdeslam, o mentor dos ataques de Paris, sendo que todos foram orquestrados pela mesma célula terrorista.

Os ataques na Bélgica foram por muitos considerados uma “tragédia anunciada” em razão do alto número de cidadãos belgas que nos anos anteriores retornaram de combates ou treinamentos na Síria e Iraque e da deficiência de recursos e pessoal de suas agências de segurança e inteligência.²²⁰ Cerca de um mês antes do evento, como parte de um plano abrangente da Casa Branca fixado após Paris para melhorar a capacidade de inteligência de aliados europeus, oficiais americanos se reuniram com autoridades belgas para cooperar no sentido de corrigir falhas em sua inteligência, especialmente sobre sua capacidade de compartilhar informações e controle de fronteiras.²²¹

A França ainda viria a suportar um novo ataque terrorista de grandes proporções em 14 de julho de 2016, data em que é comemorado o “Dia da Bastilha”, quando, ainda sob vigência do estado de emergência, um cidadão tunisiano residente na França causou a morte de 86 pessoas por atropelamento com um caminhão. Nesse caso, a inteligência francesa não detinha qualquer informação sobre o autor do ataque.

²¹⁹ BORGER, Julian. French and Belgian intelligence knew Paris attackers had jihadi backgrounds. **The Guardian**, 16 nov. 2015. Disponível em: <<http://www.theguardian.com/world/2015/nov/16/french-and-belgian-intelligence-knew-paris-attackers-had-jihadi-backgrounds>>

²²⁰ LUCE, Dan De; GROLL, Elias. In Brussels Attacks, Chronicle of a Disaster Foretold. **Foreign Policy**, 22 mar. 2016. Disponível em: <<http://foreignpolicy.com/2016/03/22/in-brussels-attacks-chronicle-of-a-disaster-foretold/>>

²²¹ SCHMITT, Eric. U.S. Officials Met With Belgians on Security Concerns Before Attacks. **The New York Times**, 4 abr. 2016. Disponível em: <<http://www.nytimes.com/2016/04/05/world/europe/us-security-brussels-attacks>>

3 CAPACIDADES E EFEITOS COLATERAIS DE ESTRATÉGIAS ABRANGENTES DE INTELIGÊNCIA

“New Collection Posture: Sniff it All – Know it All – Collect it All – Process it All – Exploit it All – Partner it All” (Documento de apresentação em conferência anual dos *Five Eyes* em 2011, descrevendo sua “nova postura de coleta” (cf. **Anexo 5**).²²²

Como se nota, o período coberto pela análise antecedente (2001-2016) evidencia um cenário de alerta e de fortalecimento de aparatos de segurança, especialmente de serviços de inteligência, em Estados atingidos por ataques terroristas. Certamente, no mesmo período, outros Estados foram igualmente vitimados por atos de mesma natureza. Índia, Paquistão, Síria, Líbano, Afeganistão, Egito, Somália e Nigéria são exemplos de países que convivem com esse tipo de ataque, cujas motivações são as mais diversas e, vale dizer, nem sempre relacionadas ao extremismo islâmico. Isso sem mencionar populações que estão à mercê de um regime autoritário doméstico, algumas vezes genocida, ou então presenciam a ocupação militar ilícita de seu território ou mesmo a agressão de forças externas opressoras – situações que muitas vezes se perduram graças a um veto no Conselho de Segurança da ONU.

Todavia, diferentemente do medo, a segurança é uma exclusividade. Qualquer Estado é capaz de instrumentalizar o medo da população como justificativa política para reforçar os aparatos de segurança do Estado, mas poucos podem concretizar esse resultado com eficiência, especialmente com reflexos significativos no seu serviço de inteligência. Com efeito, a escolha dos casos de Estados Unidos, Espanha, Reino Unido, França, Bélgica, Alemanha e Israel foi dirigida pelo critério do impacto perceptível que um ataque ou ameaça terrorista produz na ampliação das capacidades operacionais e poderes legalmente estabelecidos do serviço de inteligência de um país. É verdade que outros Estados se enquadram nesse critério e poderiam figurar na análise, mesmo orientais, como o Paquistão, que possui um excelente serviço de inteligência. O que importa, no entanto, é perceber o grande mote da política externa nesse início de século XXI, com especial apelo nos Estados

²²² GREENWALD, Glenn. **Sem lugar para se esconder**. Tradução: Fernanda Abreu. Sextante, 2014. p. 117.

Unidos e aliados mais próximos, que é a promoção da segurança diante daquilo que veem como terrorismo extremista islâmico e dos Estados que o apoiam.

Obviamente, não se questiona aqui o direito de um Estado de realizar inteligência para se defender de ataques, o que pode ser feito através de variados mecanismos de coleta, por exemplo infiltrando agentes em células terroristas, realizando sobrevoos a campos de treinamento com *drones*, ou monitorando a comunicação de indivíduos sobre os quais recaem fundadas suspeitas. Problemas surgem, no entanto, quando aparatos de inteligência, cujo aumento de poderes foi politicamente justificado num ambiente social de medo causado por ataques terroristas, se projetam sobre objetivos diversos não necessariamente relacionados à segurança nacional e de questionável licitude.

Nas seções seguintes serão discutidas as capacidades e os principais problemas associados à uma estratégia abrangente de inteligência, devida, como evidenciado no capítulo anterior, a uma cultura de emergência diante de ataques terroristas. Essa análise será estratificada em três partes: a coleta de informações privadas de particulares; a coleta de segredos de empresa; a coleta de informações classificadas pelo Estado. Essa divisão se justifica, como explicado na Introdução, em razão da diferença de natureza da informação, dos seus respectivos titulares e dos correspondentes regimes normativos de Direito Internacional em que se inserem. Em continuação, no capítulo 4, a licitude dessas atividades será analisada segundo o mesmo critério.

3.1 Coleta de informações privadas de particulares

Uma primeira manifestação dessa distorção é a coleta de informações privadas de particulares sobre os quais não recai qualquer suspeita de envolvimento com atividades ilícitas. Atualmente, esse resultado é devido à extensa capacidade de coleta de informações de agências de inteligência de sinais sobre comunicações na *internet* e em redes de telefonia celular e favorecido por uma clara tendência de aumento no fluxo de dados nesses meios.

De acordo com a *International Telecommunication Union (ITU)*, no final do ano de 2015, cerca de 3,1 bilhões de pessoas utilizava a *internet*, o que corresponde a 43% da população mundial; em 2001 esse número era de 495 milhões de pessoas, o que representava apenas 8% do total. Já o número de assinaturas de

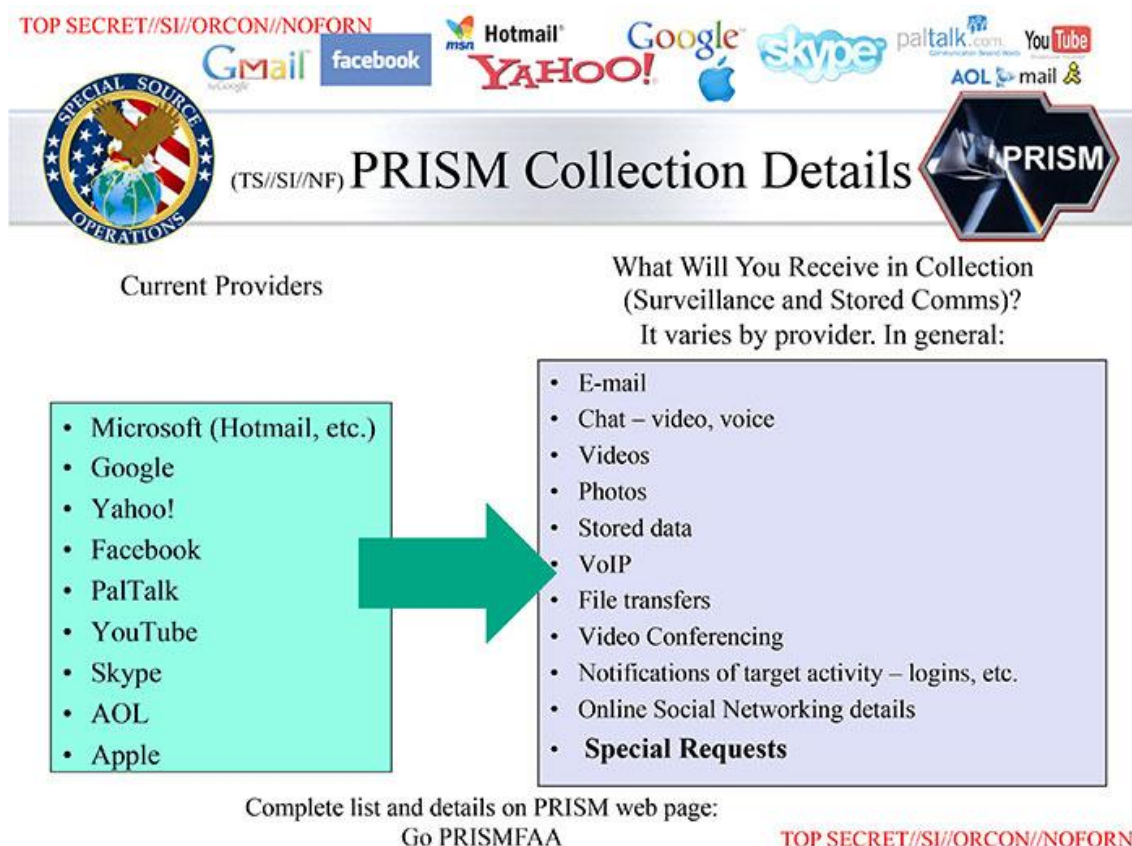
telefone celular no final de 2015 totalizava cerca de 7 bilhões.²²³ Nesse ambiente, o tráfego de informações é colossal, o que pode ser esboçado por três indicadores: a cada segundo são enviados aproximadamente 2 milhões e quatrocentos mil *e-mails* no mundo todo – apesar de aproximadamente 67% desse total ser de *spams* (propagandas) – e realizadas 1.772 (mil setecentos e setenta e duas) ligações via *Skype*.²²⁴ Além disso, dados de abril de 2014 mostravam que eram enviadas cerca de 64 bilhões de mensagens via *whatsapp* por dia.²²⁵

Como discutido na seção 1.2.2, “b”, as agências de inteligência de sinais do consórcio *Five Eyes* operam uma complexa estrutura de interceptação de informações que trafegam por cabos submarinos de fibra ótica, satélites e redes de computadores. Isso possibilita a coleta massiva de *e-mails*, mensagens de texto e de voz, vídeos, dados armazenados, entre outros, obtidos através de grandes companhias de tecnologia e seus principais serviços, como mostra abaixo o documento *top secret* de treinamento de pessoal da NSA, vazado por Snowden.

²²³ INTERNATIONAL TELECOMMUNICATION UNION. **Statistics**. Disponível em: <<http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>>

²²⁴ Estatísticas em tempo real sobre a *internet* podem ser acompanhadas em <<http://www.internetlivestats.com/>>

²²⁵ STATISTA: The Statistic Portal. **Cumulative daily mobile message volume of WhatsApp messenger as of April 2014 (in billions)**. Disponível em: <<http://www.statista.com/statistics/258743/daily-mobile-message-volume-of-whatsapp-messenger/>>



(Fonte: NSA Prism Program Slides. **The Guardian**, Disponível em: <<http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>>)

Revelações adicionais sobre o *software* de codinome XKEYSCORE, mostraram que a NSA é dotada de capacidade para obter informações de pessoas específicas, através de um nome de usuário de uma rede social, por exemplo, ou mesmo dados mais abrangentes de navegação na *internet* com um endereço de e-mail pessoal.²²⁶ Nos termos colocados por Edward Snowden em entrevista: “Sentado em minha mesa, eu certamente tinha autoridade para grampear qualquer um, de você ou seu contador até um juiz federal ou mesmo o Presidente se eu tivesse seu e-mail pessoal”.²²⁷ Posteriormente revelou-se que a NSA é dotada de capacidade de intrusão remota mesmo em computadores que não estão conectados

²²⁶ GREENWALD, Glenn. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. **The Guardian**, 31 jul. 2013. Disponível em: <<http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>>

²²⁷ “I sitting at my desk certainly had the authorities to wiretap anyone from you or your accountant to a Federal judge to even the President if I had a personal e-mail”. RODRIGUEZ, Gabriel. Edward Snowden Interview Transcript. **Policymic**, 9 jun. 2013. Disponível em: <<http://www.policymic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism>>

à *internet*, através da inserção de microtransmissores de radiofrequência em plugs de cabos *USB (Universal Serial Bus)*.²²⁸

Sabe-se também que a *NSA* possui uma operação chamada de “interrupção de cadeia de suprimento”, que consiste na interceptação de produtos de tecnologia de comunicação, como *modems* e roteadores, durante seu transporte para neles inserir ferramentas de vigilância (*backdoors*), antes que sejam enviados para clientes internacionais.²²⁹ (conferir **Anexo 6**).

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

(Fonte: GREENWALD, Glenn. **Sem lugar** ... *op. cit.* p. 142 e 258).

No documento acima, de classificação *top secret*, vazado da *NSA*, pode-se ler: “Tais Operações envolvendo interrupção de cadeia de suprimento são umas das mais produtivas operações em *TAO [Tailored Access Operations]*... Esquerda: Pacotes interceptados sendo abertos cuidadosamente: Direita: Uma “estação de carregamento’ implanta um sinalizador”.

Além do tráfego da *internet*, comunicações de telefonia celular também são monitoradas em escala massiva pela *NSA*. Um programa mais abrangente é direcionado à coleta dos metadados de ligações (por exemplo, identidade e localização dos interlocutores, duração da conversa e lista de contatos). Esse método se inicia através do número de telefone de um suspeito, o chamado “número

²²⁸ SANGER, David E.; SHANKER, Thom. N.S.A. Devises Radio Pathway Into Computers. **The New York Times**, 14 jan. 2014. <<http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html>>

²²⁹ GREENWALD, Glenn. **Sem lugar**... *op. cit.* p. 142 e 257-258.

raiz”. A partir desse número, a NSA analisa todos os outros números que receberam ou fizeram ligações para o suspeito inicial nos últimos 5 anos. Dessa forma, exemplificativamente, se o suspeito manteve contato com 100 pessoas nos últimos 5 anos, todas elas terão os metadados de suas comunicações analisados. Essa primeira expansão geométrica na base da análise é chamada de “primeiro pulo”. Se houver alguma razão para acreditar que ao menos uma dessas 100 pessoas tenha alguma ligação com um grupo terrorista, um “segundo pulo” levará à obtenção dos metadados de todos os contatos que elas mantiveram no mesmo período, a mesma lógica se aplicando ao “terceiro pulo”. Normalmente a NSA se limita ao “segundo pulo”, raras situações levando a um terceiro.²³⁰ Há ainda evidências de que a NSA colete metadados de forma indiscriminada – isto é, sem relação com uma suspeita individual. Esse tipo de operação foi exposto através do vazamento de uma decisão da FISC que determinava à empresa de telecomunicações Verizon a entrega diária de metadados à NSA de todas as ligações nas quais ao menos um dos interlocutores estivesse no território dos Estados Unidos (cf. **Anexo 4**).

Já a gravação do conteúdo da comunicação, algo mais complexo para processar, somente ocorrerá em hipóteses individualizadas: caso um dos interlocutores seja um cidadão dos Estados Unidos ou esteja no território do país é necessário um mandado judicial da FISC para a monitoração²³¹; caso a comunicação seja realizada entre pessoas de outra cidadania e que estejam fora do território dos Estados Unidos ou não se possa saber onde se situam, a gravação da comunicação é autorizada sem a necessidade de obtenção de um mandado judicial.²³² Um quadro esquemático com os parâmetros legais para a operação da SIGINT nos Estados Unidos pode ser lido no **Anexo 7**.

Diante desse cenário, algumas perguntas despertam. Inicialmente, questiona-se: ao coletar essa massiva quantidade de informação, as agências de inteligência de sinais são capazes de separar o que é relevante para a defesa nacional do que interessa apenas ao foro privado das pessoas? A verdade é que nem sempre é possível estabelecer, aprioristicamente, qual é o conteúdo da informação sem que

²³⁰ CLARKE Richard A.; MORELL, Michael J.; STONE, Geoffrey R.; SUNSTEIN, Cass R.; SWIRE, Peter. **Liberty and Security in a Changing World**: Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies, 12 dez. 2013. p. 102-103. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>

²³¹ UNITED STATES OF AMERICA. **Foreign Intelligence Surveillance Act**, sections 105; 402 e 702-705.

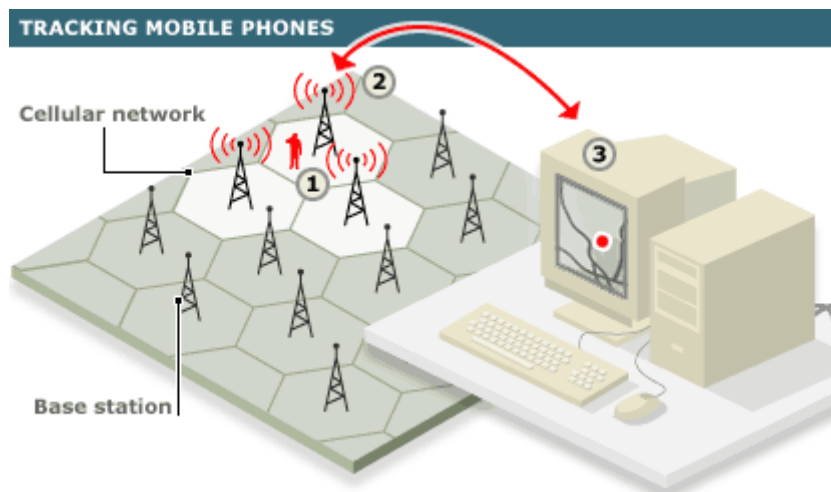
²³² UNITED STATES OF AMERICA. **Executive Order nº 12.333**.

seja ela coletada. Na maior parte do tempo as agências de inteligência fazem, por analogia, algo semelhante à garimpagem: coletar todas as informações que tem um potencial de conter algo relevante. Como ironicamente colocado por Richard Ledgett, um diretor da NSA em um evento em que foi proporcionada à agência o direito de resposta a uma participação anterior de Edward Snowden, “se nós pudéssemos fazer com que todos os sujeitos maus usassem um canto da *internet*, nós poderíamos ter um domínio sujeitomau.com. Isso seria incrível, e nós poderíamos concentrar todos nossos esforços lá”.²³³

Mas como não é possível definir com precisão e *a priori* qual é a informação de conteúdo relevante, as agências coletam quantidades massivas de comunicações, seja na *internet*, seja em redes de celulares, em forma de metadados. Sabendo então quem enviou determinado *e-mail*, ou de onde foi realizada dada ligação, além de outros padrões e filtros, a inteligência pode decidir por analisar ou não o conteúdo futuro da comunicação.

De fato, mesmo a NSA está sujeita a limitações técnicas e econômicas e não é realístico supor que ela analise o conteúdo referente a todos os metadados que coleta. O problema é que os próprios metadados já revelam muito a respeito da vida privada de alguém, a começar pelas pessoas com quem ela mais se comunica, que possivelmente serão aquelas mais próximas de sua rede de relacionamentos. Através da análise dos metadados de celulares, também é possível definir com exatidão a localização de uma pessoa em determinado horário, esteja o aparelho conectado à *internet*, pelo método de posicionamento global, ou não, através da triangulação do sinal com as antenas mais próximas.

²³³ “[...] if we could make it so that all the bad guys used one corner of the Internet, we could have a domain, badguy.com. That would be awesome, and we could just concentrate all our efforts there”. THE NSA responds to Edward Snowden’s TED Talk. **TED**, mar. 2014. Disponível em: <http://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk/transcript?language=en#t-509180>



Método de localização por triangulação

- 1) Celular envia o sinal para estações mais próximas
- 2) Softwares de posicionamento realizam o cálculo de triangulação
- 3) Os dados são convertidos em localização geográfica

(Adaptado de TRACKING a suspect by mobile phone. **BBC News**. Disponível em: <http://news.bbc.co.uk/2/hi/technology/4738219.stm>)

Metadados de atividades na *internet* poderão ainda revelar o IP (*internet protocol*), espécie de número de identificação de determinado computador e, uma vez associado à pessoa que o utiliza, é possível relacionar todos os *sites* que ela visitou em dado período. Isso sem que se analise o conteúdo de comunicações privadas.

Em suma, respondendo ao primeiro questionamento, pode-se afirmar que na coleta de metadados não é possível discriminar o valor da informação e, portanto, não é possível separar o que tem ou não valor para as operações da agência, ou seja, o relevante do trivial. Assim, adota-se uma estratégia abrangente de coleta de metadados. Uma vez identificados metadados que, em razão dos interlocutores de uma comunicação ou da localização que ela provém, entre outras formas de filtragem, evidencie alguma relevância, o conteúdo futuro da informação poderá ser analisado e assim será possível distinguir aquilo que interessa à defesa nacional.

Uma segunda questão que se coloca é a de saber se as informações privadas coletadas são armazenadas pelas agências de inteligência. A resposta é definitivamente positiva. Ocorre que aqui o mesmo raciocínio econômico de limitação de capacidade e recursos é válido: as agências não têm interesse em armazenar

informações triviais que em nada contribuem para suas atividades, gerando um custo desnecessário.

Há também restrições legais ao armazenamento das informações. Analisando o caso dos Estados Unidos, em regra, as agências de inteligência podem armazenar uma comunicação por no máximo cinco anos, havendo exceções para “inteligência estrangeira”, evidências criminais, comunicações criptografadas, ou comunicações em que todas as partes são cidadãos não americanos, entre outras.²³⁴ Nessas situações excepcionais, a informação poderá ser armazenada por tempo indefinido. Além disso, caso seja coletada alguma informação relativa a uma pessoa que tenha “uma expectativa razoável de privacidade”, caso em que um mandado judicial seria necessário para sua obtenção, e se o remetente e todos os destinatários estão localizados nos Estados Unidos, a informação deverá ser destruída, exceto se o Procurador-Geral do país determinar que esta informação indica algum risco à vida ou integridade física de alguém.²³⁵

Por fim, pode-se questionar se, mesmo diante de todas as restrições legais, as agências de inteligência se utilizam ou já se utilizaram de informações privadas para propósitos não relacionados à sua atividade fim, inclusive de natureza ilícita. A resposta a essa pergunta dependerá de interpretações do que se entende por atividade fim das agências de inteligência e quais os limites legais de sua atuação, o que sempre estará sujeito ao discurso político de opositores e apoiadores, além da interpretação judicial oficial. O potencial de fazê-lo, obviamente, sabe-se que as agências o tem.

Não se tem dúvida de que regimes ditatoriais instrumentalizam seus aparatos de inteligência como forma de controle social e as democracias eventualmente incorrerão em abusos de inteligência a depender do rigor de sua fiscalização. Nos Estados Unidos, em épocas passadas, quando a fiscalização sobre agências de inteligência e investigação eram fracas se comparadas ao controle que hoje é exercido sobre elas, o primeiro diretor do *FBI*, John Edgar Hoover, acumulou um histórico de abusos, reunindo informações privadas de políticos, personalidades e ativistas dos Estados Unidos, inclusive Martin Luther King. Covertendo a agência em sua polícia secreta, Hoover acumulou poder suficiente para pressionar autoridades

²³⁴ UNITED STATES OF AMERICA. **Foreign Intelligence Surveillance Act (FISA)**, 50 U.S. Code, § 1813, (3), (b). Disponível em: <<https://www.law.cornell.edu/uscode/text/50/1813>>

²³⁵ *Idem*, § 1806, (i).

de alto escalão sob chantagens e ameaças, o que lhe permitiu se manter como diretor da agência por 37 anos (de 1935 até 1972) – 48 anos se considerarmos que ele já era diretor do *Bureau of Investigation*, predecessor do *FBI*, desde 1924.²³⁶ Mas a verdade é que esse caso demonstra mais a sujeição de uma agência a um projeto pessoal de poder do que uma instrumentalização de um serviço de inteligência a políticas de vigilância ilícitas do Estado.

Recentemente, agora sob o sistema de fiscalização de inteligência mais sofisticado do mundo, um documento vazado da *NSA* descreve uma operação de coleta de informações de seis radicais islâmicos situados fora dos Estados Unidos, visando os descredibilizar publicamente por visualizar conteúdo sexual explícito ou “utilizar linguagem persuasiva explícita quando comunicando com garotas jovens inexperientes” (**Anexo 8**).²³⁷ Uma estratégia de combate ao terrorismo seguramente lícita segundo a legislação estadunidense, não há dúvidas.

Temores surgem quando se pensa na possibilidade de que operações deste tipo sejam utilizadas com finalidades não diretamente relacionadas ao combate ao terrorismo. Uma investigação de três meses do jornal *The Intercept*, sustentadas em documentos vazados por Edward Snowden, demonstrou que a *NSA* monitorou e-mails de proeminentes muçulmanos cidadãos norte-americanos. São eles: Asim Ghafoor, advogado, atuou em defesa de clientes em processos de terrorismo; Hooshang Amirahmadi, professor de Relações Internacionais da Universidade de Rutgers; Agha Saeed, ex-professor de Ciência Política da Universidade do Estado da Califórnia, atualmente ativista de liberdades civis de muçulmanos e palestinos; Nihad Awad, diretor executivo do Conselho sobre as Relações Americana-Islâmicas e Faisal Gill, político republicano que inclusive já serviu no Departamento de Segurança Nacional sob o governo George W. Bush.²³⁸ A legislação dos Estados Unidos prevê a necessidade de um mandado judicial da *FISC* para autorizar ações de inteligência quando a operação tiver por alvo um

²³⁶ KESSLER, Ronald. **The Bureau**: the secret history of the FBI. Macmillan, 2016. Conferir também: CHURCHILL, Ward; WALL, Jim Vander. **The COINTELPRO Papers**: Documents from the FBI's Secret Wars Against Domestic Dissent. South End Press, 1990.

²³⁷ GREENWALD, Glenn; GRIM, Ryan; GALLAGHER, Ryan. Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'. **The Huffington Post**, 26 nov. 2103. Disponível em: <http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html>

²³⁸ GREENWALD, Glenn; HUSSEIN, Murtaza. Meet the muslim-american leaders the FBI and NSA have been spying on. **The Intercept**, 9 jul. 2014. Disponível em: <<https://theintercept.com/2014/07/09/under-surveillance/>>

indivíduo localizado nos Estados Unidos. Nesse caso, não se sabe se houve autorização da Corte ou mesmo como foram utilizadas as informações obtidas através da monitoração. Por outro lado, não há também qualquer evidência pública ou investigação oficial em andamento de que qualquer destes indivíduos estejam envolvidos com atividades terroristas, direta ou indiretamente.²³⁹

3.2 Espionagem econômica

Espionagem econômica não é um fenômeno recente nem mesmo relacionado a estratégias de segurança nacional impulsionadas por ataques terroristas. No entanto, seguramente pode ser considerada uma manifestação de excesso dos poderes de inteligência estatal.

Trata-se de prática antiga. A própria China, que na Introdução foi apresentada como responsável pela maior obtenção ilícita de segredos de empresa nos Estados Unidos, historicamente, já fora vítima de notáveis casos de espionagem econômica, quando o processo de produção da seda foi assimilado pela Índia e o da porcelana pela França.²⁴⁰ Atualmente o que se nota é uma postura cada vez mais agressiva de alguns Estados com capacidade técnica de conduzir a atividade no espaço cibernético, valendo-se do rápido progresso em tecnologias da comunicação que permitem a obtenção de segredos remotamente.

O caso da China, como antecipado na Introdução, desperta preocupações mais graves no governo americano pois há um longo histórico de obtenção ilícita de segredos de empresa atribuído ao país. Mesmo após o acordo de setembro de 2015, em que Estados Unidos e China se comprometeram a não se confrontarem com atos de espionagem econômica (cf., Introdução), suas atividades ainda são consideradas pelo governo americano como “ameaças persistentes avançadas” (*Advanced Persistent Threats*)²⁴¹, termo comumente utilizado em relatórios de segurança cibernética para descrever as operações chinesas. Além disso, os cinco oficiais do Exército de Libertação Popular da China que foram acusados no judiciário

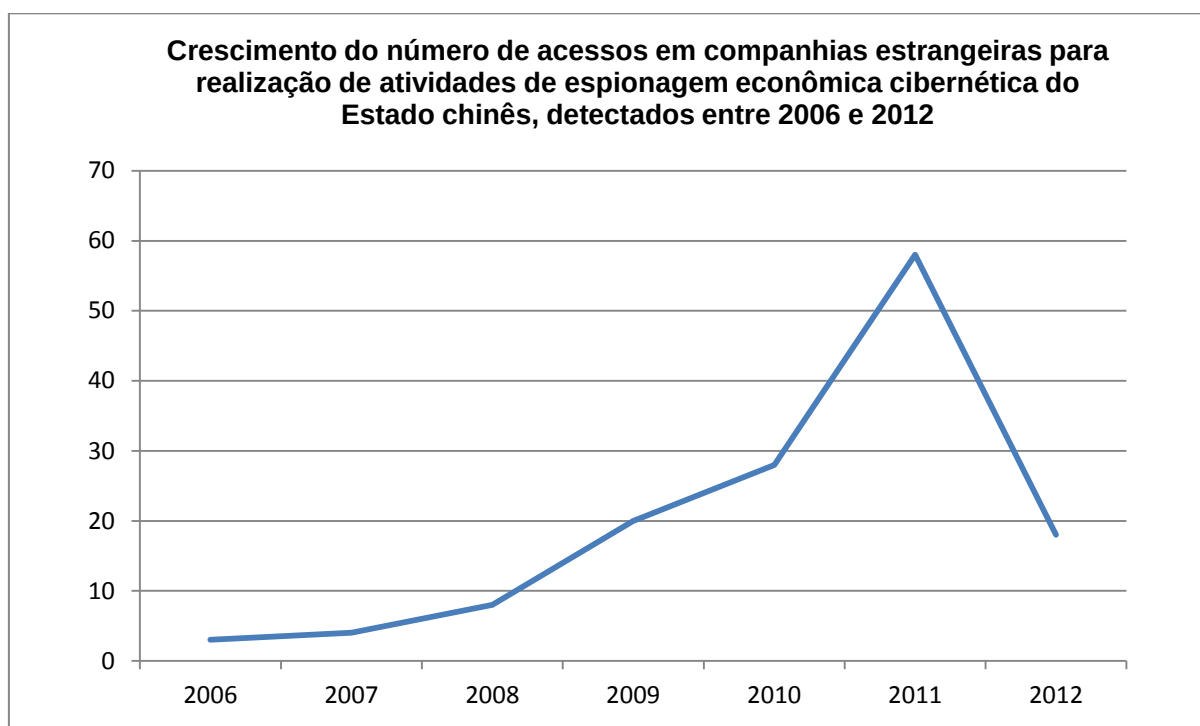
²³⁹ *Ibidem*.

²⁴⁰ BERGIER, Jacques. **Secret Armies**: The Growth of Corporate and Industrial Espionage. Tradução de Harold J. Salemson, Indianapolis: Bobbs-Merrill, 1975.

²⁴¹ DIRECTOR OF NATIONAL INTELLIGENCE. **Worldwide...** *op. cit.* p. 3.

americano por atos de espionagem econômica cibernética (cf. Introdução) ainda tem suas fotos estampadas na lista dos criminosos mais procurados pelo *FBI*.²⁴²

De fato, um relatório da companhia *Mandiant*, publicado em 2013, evidencia um crescimento exponencial das atividades de espionagem cibernética com origem em instalações do governo Chinês desde 2006 até 2011.²⁴³ Apesar de os Estados Unidos terem sido o principal alvo das operações (115 acessos), outros quatorze Estados também foram atingidos.²⁴⁴

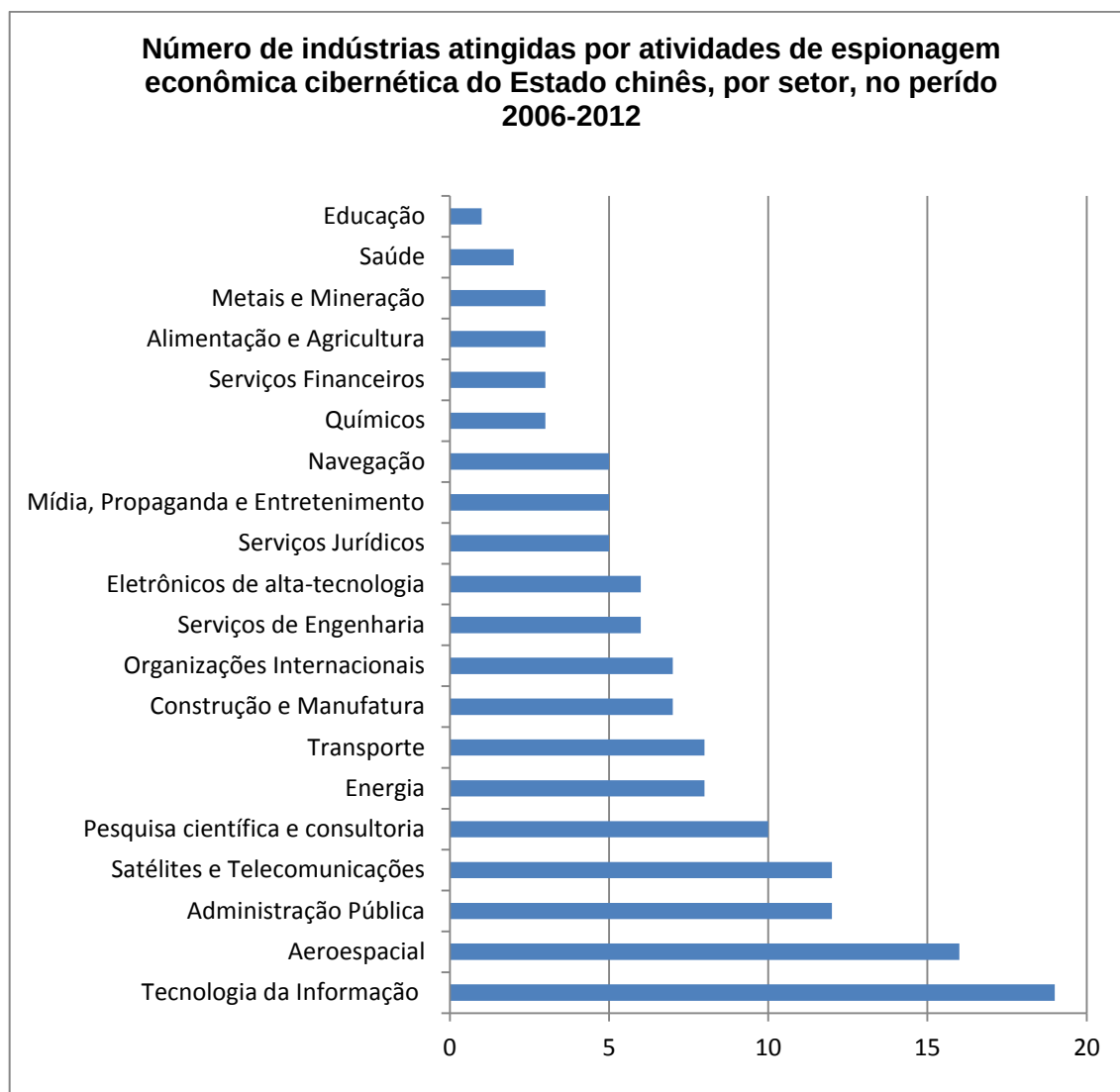


(Total: 141 acessos. Adaptado de MANDIANT. *op. cit.* p. 23).

²⁴² FEDERAL BUREAU OF INVESTIGATION. **Wanted by the FBI: Cyber's Most Wanted**. Disponível em: <<https://www.fbi.gov/wanted/cyber>>

²⁴³ Um relatório da companhia de segurança cibernética *Fire Eye* de junho de 2016 evidencia um decréscimo significativo nas operações de intrusão cibernética chinesa a partir de 2014, o que se atribui a reformas militares por que vem passando o país e à larga exposição das atividades em razão dos protestos do governo norte-americano. Cf. FIREEYE. **Red Line Drawn: China recalculates its use of cyber espionage**, jun. 2016. Disponível em: <<https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf>>

²⁴⁴ MANDIANT. *op. cit.* p. 22.



(Adaptado de MANDIANT. *op. cit.* p. 24)

Os dados obtidos através dos acessos clandestinos referem-se a desenvolvimento de produtos, incluindo informações sobre testes e manuais, *design* de sistemas, tecnologias de simulação, processos industriais, planos de negócios, informações sobre contratos e posições em negociações, métodos de precificação de produtos, informações jurídicas e informações sobre fusões e aquisições.²⁴⁵

Além da China, o Irã, a Coreia do Norte e a Rússia também são vistos como ameaças centrais à segurança cibernética norte-americana, esta última que, inclusive, está implementando um “comando cibernético” junto a seu Ministério da Defesa, com capacidade para conduzir “operações cibernéticas ofensivas”.²⁴⁶

²⁴⁵ MANDIANT. *op. cit.* p. 25.

²⁴⁶ DIRECTOR OF NATIONAL INTELLIGENCE. **Worldwide Threat...** *op. cit.* p. 2-3.

De outro lado, há fortes motivos para crer que a NSA também conduz operações de espionagem econômica cibernética. Como afirmado na Introdução, o nome da *Petrobras* é mencionado em um documento da agência como alvo de espionagem (cf. **Anexo 9**). Acresça-se a isso revelações de que a agência canadense de inteligência de sinais, a *Communications Security Establishment* (CSE), uma associada dos Estados Unidos no Consórcio *Five Eyes*, teve como alvo de uma de suas operações (codinome *Olympia*), o Ministério das Minas e Energia do Brasil (cf. **Anexo 10**).

Ainda que não se saiba exatamente quais informações foram obtidas nessas operações, há razões para se acreditar que envolvam segredo de empresa. Especulou-se na imprensa que a operação “*Olympia*” tenha ligações com o leilão, designado para o dia 21 de outubro de 2013, da concessão para exploração do “Campo de Libra”, região do mar territorial brasileiro que abarca o maior volume de “petróleo pré-sal” já descoberto, notando o fato de que nenhuma das grandes empresas exploradoras de petróleo sediadas nos países do grupo *five eyes* se inscreveram para o leilão.^{247 248} Observou-se também que mais de 40 companhias de mineração canadense operam no Brasil, setor em que os dois países são rivais no mercado internacional, além da aviação, exploração de petróleo e agricultura.²⁴⁹

Apesar de porta-vozes do governo e da NSA afirmarem insistentemente que a inteligência dos Estados Unidos não realiza espionagem econômica²⁵⁰, duas outras

²⁴⁷ FITZ-MORRIS, James. Why would Canada spy on Brazil mining and energy officials? **CBC News**, 09 out. 2013. Disponível em: <<http://www.cbc.ca/news/politics/why-would-canada-spy-on-brazil-mining-and-energy-officials-1.1931465>>

²⁴⁸ Estavam inscritas para o leilão as empresas CNOOC International Limited (China), China National Petroleum Corporation (China), Ecopetrol (Colômbia), Mitsui & CO (Japão), ONGC Videsh (Índia), Petrogal (Portugal), Petrobras (Brasil), Petronas (Malásia), Repsol/Sinopec (hispano-chinesa), Shell (anglo-holandesa) e Total (França). Curiosamente as petroleiras norte-americanas Chevron e Exxon Mobil e as britânicas BP e BG não participaram da disputa. Ao final o leilão foi vencido pelo consórcio liderado por Petrobras (40%), Shell (20%), Total (20%) e as chinesas CNPC e CNOOC (10% cada). VALLE, Sabrina; BAHNEMANN, Wellington; CIARELLI, Mônica. Sem disputa, Petrobras vence leilão de Libra com Shell, Total e duas chinesas. **Agência Estado**, 21 out. 2013. Disponível em: <<http://economia.estadao.com.br/noticias/geral,sem-disputa-petrobras-vence-leilao-de-libra-com-shell-total-e-duas-chinesas,168014e>>

²⁴⁹ ISMI, Asad. Canadian government spies on Brazil – and its own citizens. **Canadian Center for Policy Alternatives**, 1 nov. 2013. Disponível em: <<https://www.policyalternatives.ca/publications/monitor/massive-secret-surveillance-canada>>

²⁵⁰ “The department [of defense] does not engage in economic espionage in any domain, including cyber”, foi o que afirmou um porta-voz da NSA ao jornal *The Washington Post*. GELLMAN, Barton; NAKASHIMA, Ellen. U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show. **The Washington Post**, 30 ago. 2013. Disponível em: <https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html>

revelações desautorizam a escusa. A primeira diz respeito à estratégia de contenção da empresa chinesa *Huawei* – uma das maiores companhias de tecnologia de comunicação do mundo – com o objetivo de evitar seu ingresso no mercado norte-americano – tarefa bem sucedida até o momento. Além da companhia chinesa ser concorrente direta da americana *Cisco* e de ser prejudicada por estratégias protecionistas nos Estados Unidos e países aliados²⁵¹, há um temor de que a entrada de *modems*, celulares e outros aparelhos de comunicação *Huawei* no mercado norte-americano possa ampliar as capacidades de SIGINT do Exército de Libertação Popular, com que acredita-se que a companhia possua laços.²⁵² Nesse contexto, a *Huawei* se tornou um alvo prioritário da NSA, que através da operação de codinome “*Shotgiant*”, obteve uma lista com 1.400 contatos de consumidores da empresa, documentos de treinamento de engenheiros para utilização de produtos *Huawei* e, mais grave, o código-fonte dos produtos²⁵³ – todas informações consideradas segredo de empresa.

Comentando as revelações da espionagem sobre a *Huawei*, Jack Goldsmith declarou:

As revelações *Huawei* são refutações devastadoras das reclamações hipócritas dos Estados Unidos sobre a penetração chinesa em suas redes, e fazem com que as alegações do governo sobre não subtrair propriedade intelectual para ajudar a competitividade de empresas norte-americanas pareçam a conveniente distinção que de fato são.²⁵⁴

As alegações do governo americano de que sua inteligência não conduz espionagem econômica se enfraqueceram ainda mais em 2015, quando o portal *wikileaks* publicou uma série de documentos classificados denunciando que a

²⁵¹ Em 2010 e 2013, os Estados Unidos persuadiram a Austrália e a Coreia do Sul, respectivamente, a desistirem de negociações com a *Huawei* envolvendo contratos para construção de redes de telecomunicação. Cf. SANGER, David E.; PERLROTH, Nicole. N.S.A. Breached Chinese Servers Seen as Security Threat. **The New York Times**, 22 mar. 2014. Disponível em: <http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?hp&_r=0>

²⁵² *Ibidem*.

²⁵³ TARGETING Huawei: NSA Spied on Chinese Government and Networking Firm. **Spiegel Online International**, 22 mar. 2014. Disponível em: <<http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html>>

²⁵⁴ “The Huawei revelations are devastating rebuttals to hypocritical U.S. complaints about Chinese penetration of U.S. networks, and also make USG protestations about not stealing intellectual property to help U.S. firms’ competitiveness seem like the self-serving hairsplitting that it is”. GOLDSMITH, Jack. The NYT on NSA’s Huawei Penetration. **Lawfare**, 22 mar. 2014. Disponível em: <<https://www.lawfareblog.com/nyt-nssas-huawei-penetration-updated>>

França foi alvo de operações de vigilância da NSA. Segundo um dos documentos, a agência foi orientada a coletar, entre outras informações, dados sobre as relações econômicas do país com os Estados Unidos; práticas negociais francesas; contratos e negociações francesas com estrangeiros; política comercial e atividades comerciais “questionáveis” da França. Entre os destinatários das informações encontram-se, além da CIA, da DIA, e do DHS, o Departamento de Comércio (*U.S. Department of Commerce*), o Escritório do Representante de Comércio (*Office of the U.S. Trade Representative*) e o Departamento do Tesouro.²⁵⁵ Outro documento demonstra que a NSA foi instruída a relatar contratos e negociações exteriores da França que sejam de “significante interesse” para um Estado estrangeiro contraparte ou que representem um valor de 200 milhões de dólares ou mais, com especial foco em áreas de tecnologia de comunicação e informação, energia, infraestrutura e tecnologia de transportes, tecnologias de meio-ambiente, saúde e biotecnologia.²⁵⁶

3.3 Espionagem de informações classificadas

A espionagem de informações classificadas, ou “segredos de Estado”, é a essência da inteligência. Um serviço de inteligência que se limitasse à obtenção de informações publicamente disponíveis se mostraria pouco eficiente, incapaz de informar adequadamente as autoridades políticas e militares das reais nuances que podem afetar sua tomada de decisão. De fato, as informações que são mais sensíveis do ponto de vista estratégico são aquelas que os Estados ocultam uns dos outros, o que implica também ocultá-las do público em geral. Para isso existe o sistema de classificação de informações, brevemente discutido na seção 1.2.5.

Seguindo esse raciocínio, um Estado que deseje obter informação classificada de outro Estado irá conduzir uma operação clandestina, pois caso o detentor da informação identifique uma tentativa de coleta – por consequência frustrada – fará aumentar o rigor de sua proteção ou implantará informações falsas destinadas a enganar o coletor (*deception operation*). Isso reduziria as chances de obter a informação além de fazer com que o Estado que conduziu a operação

²⁵⁵ ESPIONNAGE Élysée. **Wikileaks**, 23 jun. 2015. Disponível em <<https://www.wikileaks.org/nsa-france/spyorder/>>

²⁵⁶ *Ibidem*.

tivesse que lidar com as consequências políticas deletérias do ato que, ao menos no plano retórico, encontraria voraz oposição do Estado alvo.

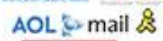
Portanto, os Estados que se preocupam com sua posição estratégica no cenário global irão desenvolver técnicas clandestinas de coleta, sendo bem sucedidos na tarefa em maior ou menor grau, de acordo com diversos fatores que podem incluir sua condição econômica, competência técnica, criatividade para desenvolver métodos de intrusão e presença de oficiais no território de outros países. Os Estados Unidos, por exemplo, conseguem realizar com sucesso operações de SIGINT por uma combinação de fatores: distinta capacidade tecnológica de agências do governo e de empresas, forte presença de mercado de suas companhias de tecnologia, o que permite acesso a variados meios de comunicação no mundo todo (satélites, servidores, *modems*, roteadores, celulares, *tablets*, *laptops* etc.) e participação em redes de compartilhamento de inteligência.

Uma boa ilustração dessa capacidade pode ser vista no documento abaixo, material de treinamento vazado da NSA, em que se mostra que a maior parte das comunicações do mundo é transmitida para ou através dos Estados Unidos.

TOP SECRET//SI//ORCON//NOFORN



Hotmail®

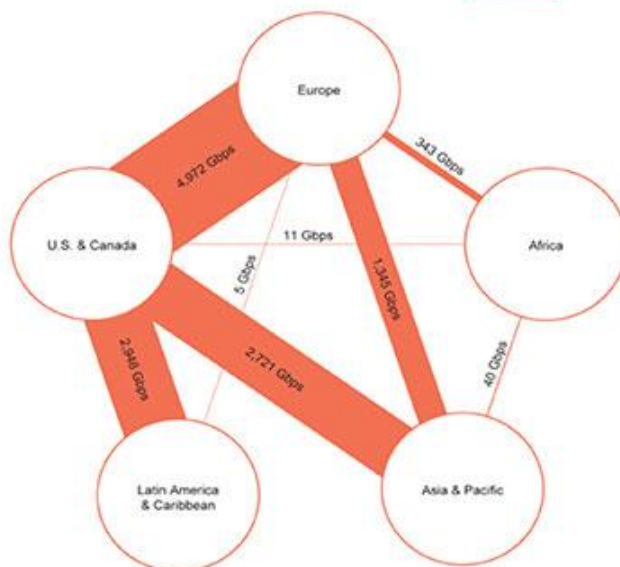


(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone



- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



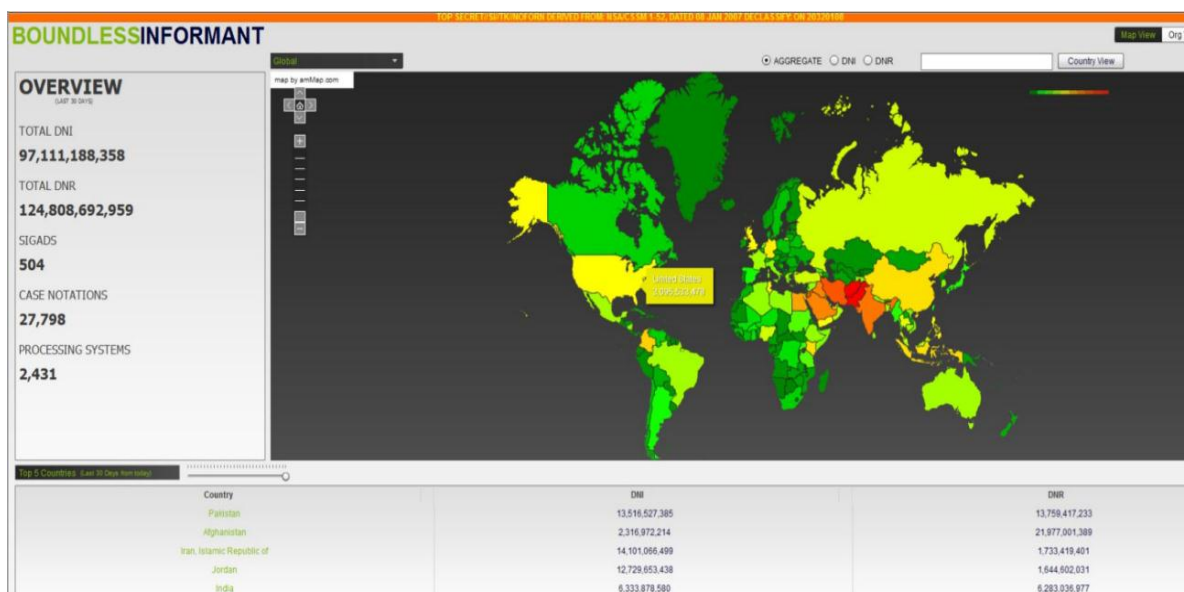
International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

(Fonte: THE GUARDIAN. NSA Prism Program Slides. Disponível em: <http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>>)

O recebimento da maior parte das comunicações digitais em servidores localizados em seu território, juntamente com acessos obtidos em outros Estados, proporcionam à inteligência de sinais dos Estados Unidos abrangência global, como mostra uma imagem de utilização da ferramenta de análise *Boundless Informant*, da NSA (melhor visualizado no **Anexo 11**).



(Fonte: GREENWALD, Glenn; MACKASKILL, Ewen. Boundless Informant: the NSA's secret tool to track global surveillance data, **The Guardian**, 11 jun. 2013. Disponível em: <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>>)

Como se lê no documento, em um período de 30 dias a partir de 8 de março de 2013, a unidade de operações de acesso global da NSA (*Global Access Operation – GAO*), obteve metadados de mais de 97 bilhões de *DNI* (*Digital Network Intelligence*; Inteligência de Redes Digitais) e mais de 124 bilhões de *DNR* (*Dialed Number Recognition*; Reconhecimento de Ligações Telefônicas) no mundo todo.²⁵⁷ Obviamente, apenas uma pequena parcela disso deve envolver segredos de Estado sendo a maior parte referente a comunicações privadas.

Não obstante, o documento revela outras informações interessantes que permitem observar quais países eram alvos prioritários da inteligência de sinais norte-americana naquele momento. Em grau máximo Paquistão e Afeganistão eram os Estados mais sujeitos à vigilância. Em um segundo patamar, Índia, Irã, Iraque, Arábia Saudita, Egito e Jordânia. Em terceiro, nota-se que a vigilância exercida sobre China e Alemanha era de mesmo nível que a realizada no Reino Unido e internamente nos próprios Estados Unidos. Possivelmente, Rússia e China hoje devem receber maior atenção da inteligência norte-americana do que em 2013, em razão de recentes movimentos de expansão territorial, respectivamente, sobre a Crimeia, elevando a preocupação de Estados da OTAN, e sobre ilhas do mar do sul da China, também reivindicadas por Vietnam, Malásia, Indonésia, Taiwan e Brunei, aliados dos Estados Unidos.

²⁵⁷ GREENWALD, G. **Sem Lugar...** op. cit. p. 95.

As informações classificadas alvo da espionagem estatal podem proporcionar uma equiparação ou uma vantagem estratégica ao Estado que as coletam em relação aos rivais, o que fica especialmente claro nos domínios militar, político e diplomático. O exemplo em que a espionagem produziu os reflexos mais decisivos em termos militares e geopolíticos talvez seja a obtenção de informações relacionadas ao processo de produção da bomba atômica por espiões soviéticos posicionados nos Estados Unidos e no Reino Unido. Apesar de o processo de fissão nuclear ser de conhecimento da comunidade científica mesmo antes do início da segunda guerra mundial, a União Soviética experimentava diversas dificuldades de natureza técnica que iam desde o refinamento do urânio ao mecanismo de detonação da bomba. Fruto de um dedicado esforço, a inteligência soviética conseguiu infiltrar habilidosos espiões no Projeto *Tube Alloys* – empreitada britânica para a construção da bomba atômica – e no Projeto *Manhattan* – sua contraparte norte-americana que realizou o primeiro teste de explosão atômica da história, em *Alamogordo*, estado do Novo México. Entre os chamados *Atomic Spies* envolvidos no Projeto *Manhattan* estão Klaus Fuchs, alemão a serviço do GRU, Theodore Hall, americano, que se voluntariou para repassar informações à União Soviética e David Greenglass, também americano, recrutado pela KGB – todos eles de inclinação comunista.²⁵⁸ Estima-se que a União Soviética iria conseguir construir a bomba atômica mesmo sem o auxílio da espionagem, que teria acelerado o objetivo, entretanto, em 12 a 18 meses.²⁵⁹ De qualquer forma, em 29 de agosto de 1949, quatro anos após os ataques a *Hiroshima* e *Nagasaki* (respectivamente em 6 e 9 de agosto de 1945), a União Soviética conduzia seu primeiro teste de explosão de uma bomba nuclear, cujo dispositivo era uma cópia exata do utilizado nos testes do Projeto *Manhattan*.^{260 261}

Desde a década de 1990, informações mostram que a China é agressiva também em direção a tecnologias militares, paralelamente às recentes investidas

²⁵⁸ Conferir o capítulo 5 de HAYNES, John Earl; KLHER, Harvey. **Early Cold War Spies**. Cambridge University Press, 2006. p. 138 e seguintes. Conferir também RICHELSON, Jeffrey T. **A Century of Spies: Intelligence in the Twentieth Century**. Oxford University Press, 1995. p. 134-139.

²⁵⁹ HOLLOWAY, David. *Stalin and the Bomb: The Soviet Union and Atomic Energy, 1939-1956*. Yale University Press, 1994. p. 222.

²⁶⁰ ANDREW, Christopher; MITHROKIN, Vasili. **The Sword and the Shield: The Mitrokhin Archive and the Secret History of KGB**. Basic Books, 1995. p. 132.

²⁶¹ As conclusões oficiais do governo norte-americano acerca da espionagem soviética sobre seu programa nuclear podem ser lidas em: JOINT COMMITTEE ON ATOMIC ENERGY. **Soviet Atomic Espionage**, 1951. Disponível em: <http://archive.org/stream/sovietatomicespionage1951unit#page/n4/mode/1up>

nos segredos de empresa. Desde então, sabe-se que informações sobre os bombardeiros B-1, o *stealth* B-2, o sistema de propulsão submarina “*Quiet Eletric Drive*” e o sistema W-88 de construção de pequenas ogivas nucleares transportadas em submarinos foram repassadas a Pequim por espões posicionados nos Estados Unidos.²⁶² Acredita-se ainda que os destroços do helicóptero *stealth Black Hawk* abatido na incursão que resultou na morte de Usama Bin Ladin em *Abbottabad*, no Paquistão, em 2 de maio de 2011 (operação *Neptune Spear*), foram inspecionados por oficiais chineses sob autorização do governo paquistanês.²⁶³

Em acréscimo, entre os documentos vazados por Edward Snowden há informações de que a China obteve sucesso em mais de 500 intrusões em sistemas do Departamento de Defesa dos Estados Unidos, obtendo ainda sensíveis informações da Força Aérea e da Marinha, incluindo dados sobre o caça de última geração F-35, sistemas de navegação de mísseis e submarinos nucleares. Estima-se que a quantidade de dados subtraídos seja de 50 *Terabytes*, o que contém o equivalente de informações a aproximadamente cinco bibliotecas do Congresso norte-americano (**Anexo 12**)²⁶⁴ – a maior biblioteca do mundo.

Mais recentemente, a publicação de um vídeo em uma rede social chinesa mostrando o lançamento do *drone* chinês *Caihong-4*, fez notar uma semelhança significativa da aeronave com os análogos norte-americanos, reforçando suspeitas de apropriação de tecnologias militares.²⁶⁵

Se segredos militares possuem um valor evidente para a defesa nacional, por vezes com reflexos significativos na balança de poder global, informações políticas sigilosas guardam expressivo valor estratégico para o desempenho da política externa, e por isso também serão alvo de operações de espionagem das agências de inteligência de Estado. Como em um jogo de *Poker*, na política internacional as apostas são altas, e é interessante saber se os adversários estão realmente dispostos a correr riscos como aparentam estar, se estão ou não blefando. Imagine então se puder ver suas cartas!

²⁶² WISE, David. China's Spies are Catching Up. **The New York Times**, 10 dez. 2011. Disponível em: <<http://www.nytimes.com/2011/12/11/opinion/sunday/chinas-spies-are-catching-up.html>>

²⁶³ MAZZETTI, Mark. U.S. Aides Believe China Examined Stealth Copter. **The New York Times**, 14 ago. 2011. Disponível em: <<http://www.nytimes.com/2011/08/15/world/asia/15copter.html>>

²⁶⁴ Os documentos podem ser encontrados na *internet* em: <<https://fveydocs.org/document/chinese-exfil-military-tech/>>

²⁶⁵ GERTZ, Bill. China's armed drones appear built from stolen data from US cyber intrusions. **Asia Times**, 29 dez. 2015. Disponível em: <<http://atimes.com/2015/12/chinas-armed-drones-appear-built-from-stolen-data-from-us-cyber-intrusions/>>

Sabe-se que comunicações privadas de líderes de Estado são alvos costumeiros da espionagem da NSA. Há documentos que comprovam que a Chanceler alemã Angela Merkel (Introdução), a Presidente brasileira Dilma Rousseff, o Presidente mexicano Enrique Peña Nieto (**Anexo 13**) e três presidentes franceses (François Hollande, Nicolas Sarkozy e Jacques Chirac) foram sujeitos à vigilância da inteligência dos Estados Unidos.²⁶⁶ No caso da Presidente brasileira, o esforço da espionagem era direcionado à compreensão dos métodos de comunicação da chefe do executivo com seus principais conselheiros, como se lê no documento abaixo.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C42 surge effort

(U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.



TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(Fonte: FVEYDOCS.ORG. **A number of NSA slides released by the Brazilian publisher O Globo that describe NSA surveillance of then Mexican presidential candidate Enrique Pena Nieto and Brazilian president Dilma Rousseff.** Disponível em: <<https://fveydocs.org/document/intelligently-filtering-your-data-brazil-and-mexico-case-studies/>>)

Além de líderes de Estado, a inteligência norte-americana também tem por alvo comunicações diplomáticas, que servirão de subsídios para o exercício da política externa do país. Um documento datado de setembro de 2010 lista as

²⁶⁶ WIKILEAKS. **Espionnage...** op. cit. Disponível em <<https://www.wikileaks.org/nsa-france/intercepts/#intercept2>>

embaixadas e representações estrangeiras sediadas nos Estados Unidos cujos sistemas foram comprometidos por operações da NSA.

10 Sep 2010				
CLOSE ACCESS SIGADS				
CLOSE ACCESS SIGADS				
All Close Access domestic collection uses the US-3136 SIGAD with a unique two-letter suffix for each target location and mission. Close Access overseas GENIE collection has been assigned the US-3137 SIGAD with a two-letter suffix.				
(Note: Targets marked with an * have either been dropped or are slated to be dropped in the near future. Please check with TAO/RTD/ROS (961-1578s) regarding authorities status.)				
SIGAD US-3136				
SUFFIX	TARGET/COUNTRY	LOCATION	COVERTERM	MISSION
BE	Brazil/Emb	Wash,DC	KATEEL	LIFESAVER
SI	Brazil/Emb	Wash,DC	KATEEL	HIGHLANDS
VQ	Brazil/UN	New York	POCOMOKE	HIGHLANDS
HN	Brazil/UN	New York	POCOMOKE	VAGRANT
LJ	Brazil/UN	New York	POCOMOKE	LIFESAVER
YL *	Bulgaria/Emb	Wash, DC	MERCED	HIGHLANDS
QX *	Colombia/Trade Bureau	New York	BANISTER	LIFESAVER
DJ	EU/UN	New York	PERDIDO	HIGHLANDS
SS	EU/UN	New York	PERDIDO	LIFESAVER
KD	EU/Emb	Wash, DC	MAGOTHY	HIGHLANDS
IO	EU/Emb	Wash, DC	MAGOTHY	MINERALIZ
XJ	EU/Emb	Wash,DC	MAGOTHY	DROPMIRE
OF	France/UN	New York	BLACKFOOT	HIGHLANDS
VC	France/UN	New York	BLACKFOOT	VAGRANT
UC	France/Emb	Wash, DC	WABASH	HIGHLANDS
LO	France/Emb	Wash, DC	WABASH	PBX
NK *	Georgia/Emb	Wash, DC	NAVARRO	HIGHLANDS
BY *	Georgia/Emb	Wash, DC	NAVARRO	VAGRANT
RX	Greece/UN	New York	POWELL	HIGHLANDS
HB	Greece/UN	New York	POWELL	LIFESAVER
CD	Greece/Emb	Wash, DC	KLONDIKE	HIGHLANDS
PJ	Greece/Emb	Wash,DC	KLONDIKE	LIFESAVER

JN	Greece/Emb	Wash, DC	KLONDIKE	PBX
MO *	India/UN	New York	NASHUA	HIGHLANDS
QL *	India/UN	New York	NASHUA	MAGNETIC
ON *	India/UN	New York	NASHUA	VAGRANT
IS *	India/UN	New York	NASHUA	LIFESAVER
OX *	India/Emb	Wash, DC	OSAGE	LIFESAVER
CQ *	India/Emb	Wash, DC	OSAGE	HIGHLANDS
TQ *	India/Emb	Wash, DC	OSAGE	VAGRANT
CU *	India/EmbAnx	Wash, DC	OSWAYO	VAGRANT
DS *	India/EmbAnx	Wash, DC	OSWAYO	HIGHLANDS
SU *	Italy/Emb	Wash, DC	BRUNEAU	LIFESAVER
MV *	Italy/Emb	Wash, DC	HEMLOCK	HIGHLANDS
IP *	Japan/UN	New York	MULBERRY	MINERALIZ
HF *	Japan/UN	New York	MULBERRY	HIGHLANDS
BT *	Japan/UN	New York	MULBERRY	MAGNETIC
RU *	Japan/UN	New York	MULBERRY	VAGRANT
LM *	Mexico/UN	New York	ALAMITO	LIFESAVER
UX *	Slovakia/Emb	Wash, DC	FLEMING	HIGHLANDS
SA *	Slovakia/Emb	Wash, DC	FLEMING	VAGRANT
XR *	South Africa/ UN & Consulate	New York	DOBIE	HIGHLANDS
RJ *	South Africa/ UN & Consulate	New York	DOBIE	VAGRANT
YR *	South Korea/UN	New York	SULPHUR	VAGRANT
TZ *	Taiwan/TECO	New York	REQUETTE	VAGRANT
VN *	Venezuela/Emb	Wash, DC	YUKON	LIFESAVER
UR *	Venezuela/UN	New York	WESTPORT	LIFESAVER
NO *	Vietnam/UN	New York	NAVAJO	HIGHLANDS
OU *	Vietnam/UN	New York	NAVAJO	VAGRANT
GV *	Vietnam/Emb	Wash, DC	PANTHER	HIGHLANDS

SIGAD US-3137

GENERAL TERM DESCRIPTIONS

HIGHLANDS: Collection from Implants

VAGRANT: Collection of Computer Screens

MAGNETIC: Sensor Collection of Magnetic Emanations

MINERALIZE: Collection from LAN Implant

OCEAN: Optical Collection System for Raster-Based Computer Screens

LIFESAVER: Imaging of the Hard Drive

GENIE: Multi-stage operation; jumping the airgap etc.

BLACKHEART: Collection from an FBI Implant

PBX: Public Branch Exchange Switch

CRYPTO ENABLED: Collection derived from AO's efforts to enable crypto

DROPMIRE: passive collection of emanations using an antenna

CUSTOMS: Customs opportunities (not LIFESAVER)

DROPMIRE: Laser printer collection, purely proximal access (**NOT** implanted)

DEWSWEEPER: USB (Universal Serial Bus) hardware host tap that provides COVERT link over USB link into a target network. Operates w/RF relay subsystem to provide wireless Bridge into target network.

RADON: Bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-directional exploitation of Denied networks using standard on-net tools.

(Fonte: FVEYDOCS.ORG. Close Access SIGADs. Disponível em:
<https://fveydocs.org/document/close-access-sigads/?page=1>)

Como se lê no documento, tanto a embaixada do Brasil em Washington D.C. e a representação brasileira junto à ONU em Nova York foram espionadas pela NSA, o mesmo acontecendo com as embaixadas e representações de União Europeia, França, Itália, Japão entre outros muitos Estados.

Um interessante exemplo de como informações de natureza política e diplomática são utilizadas no exercício da política externa norte-americana ocorreu no processo de votação da Resolução 1929 do Conselho de Segurança da ONU de 09 de junho de 2010, que agora pode ser apreciado com outros olhos. A Resolução propunha seis rodadas de sanções ao Irã, instaurando um embargo de compra de armas e tecnologia nuclear e sujeitando-o a um novo regime de inspeção mais rigoroso.²⁶⁷ Segundo o documento da NSA intitulado “Sucesso silencioso: sinergia em SIGINT ajuda a moldar a política externa dos Estados Unidos” (reproduzido abaixo), durante as negociações da Resolução, a Agência realizou coleta de informações contra a representação da França, Japão, México e Brasil – os últimos três, membros não permanentes do Conselho de Segurança ao momento – fornecendo informações à embaixadora dos Estados Unidos na ONU, Susan Rice – codinomeada no documento como USUN – que lhe permitiram saber como outros Estados iriam votar.

Nas palavras com tom de gratidão da embaixadora, a inteligência de sinais:

[...] me ajudou a saber quando os outros *Permpres* [representantes permanentes do Conselho de Segurança] estavam dizendo a verdade [...] revelaram sua real posição sobre as sanções [...] nos deu uma vantagem nas negociações e proveu informações sobre o limite que os vários países estavam dispostos a aceitar.

²⁶⁷ UNITED NATIONS. **Security Council Imposes Additional Sanctions on Iran, Voting 12 in Favour to 2 Against, with 1 Abstention**. Press Release. 9 jun. 2010. Disponível em: <<http://www.un.org/press/en/2010/sc9948.doc.htm>>

TOP SECRET//COMINT//NOFORN

August 2010



(U//FOUO) Silent Success: SIGINT Synergy Helps Shape US Foreign Policy

(TS//SI//NF) At the outset of these lengthy negotiations, NSA had sustained collection against Japan, Mexico, Brazil France

(TS//SI//REL) In late spring 2010, eleven branches across five Product Lines teamed with NSA enablers to provide the most current and accurate information to USUN and other customers on how UNSC members would vote on the Iran Sanctions Resolution. Noting that Iran continued its non-compliance with previous UNSC resolutions concerning its nuclear program, the UN imposed further sanctions on 9 June 2010. SIGINT was key in keeping USUN informed of how the other members of the UNSC would vote.

(TS//SI//REL) In late spring 2010, eleven branches across five Product Lines teamed with NSA enablers to provide the most current and accurate information to USUN and other customers on how UNSC members would vote on the Iran Sanctions Resolution. Noting that Iran continued its non-compliance with previous UNSC resolutions concerning its nuclear program, the UN imposed further sanctions on 9 June 2010. SIGINT was key in keeping USUN informed of how the other members of the UNSC would vote.

(TS//SI//REL) The resolution was adopted by twelve votes for, two against (Brazil and Turkey), and one abstention from Lebanon. According to USUN, SIGINT "helped me to know when the other Permreps [Permanent Representatives] were telling the truth.... revealed their real position on sanctions... gave us an upper hand in negotiations... and provided information on various countries 'red lines.'"

(Fonte: GREENWALD, G. **Sem Lugar...** p. 256)

Também teve razões para expressar gratidão à inteligência de sinais o então Secretário de Estado Assistente Thomas Shannon que, em 2009, por ocasião da Quinta Cúpula das Américas, recebeu mais de cem relatórios da NSA que, segundo ele:

[...] nos proporcionaram uma profunda compreensão dos planos e intenções dos outros participantes da Cúpula e garantiram que nossos diplomatas estivessem bem preparados para aconselhar o presidente Obama e a secretária Clinton na condução de questões controversas, como, por exemplo, Cuba, e na interação com interlocutores difíceis como o presidente venezuelano Chávez.²⁶⁸

²⁶⁸ Em carta ao então Diretor da NSA, General Keith Alexander, o Secretário de Estado Assistente declarou: "The more than 100 reports we received from the NSA gave us deep insight into the plans and intentions of other Summit participants, and ensured that our diplomats were well prepared to advise President Obama and Secretary Clinton on how to deal with contentious issues,

Um novo e recente vazamento publicado no portal *wikileaks* contém diversos documentos altamente secretos que denunciam a vigilância da NSA sobre o telefone pessoal de agentes oficiais de organizações internacionais. Dentre eles incluem-se o Chefe de Pessoal do Alto Comissariado da ONU para os Refugiados; o Diretor da Divisão Jurídica da Organização Mundial do Comércio (OMC); cinco oficiais da União Europeia e o representante da Itália na OTAN.²⁶⁹ Conversas entre a chanceler alemã Angela Merkel e o ex-Secretário-Geral da ONU Ban Ki-Moon envolvendo futuras negociações sobre mudanças climáticas também foram interceptadas pela NSA. Além disso, a agência obteve documentos diplomáticos italianos datados de 2010 que relatavam um pedido de ajuda do premiê israelense Benjamin Netanyahu ao então primeiro-ministro italiano Silvio Berlusconi, para que este atuasse no sentido de reaproximar o governo dos Estados Unidos de Israel.²⁷⁰

such as Cuba, and interact with difficult counterparts, such as Venezuelan President Chavez". GREENWALD, G. Sem Lugar... p. 131 e 254.

²⁶⁹ NSA Targets World Leaders for US Geopolitical Interests. **Wikileaks**, Disponível em: <<https://www.wikileaks.org/nsa-201602/>>

²⁷⁰ *Ibidem*.

4 ANALISANDO A LICITUDE DAS ATIVIDADES DE ESPIONAGEM NO DIREITO INTERNACIONAL²⁷¹

“International legal discourse is incoherent as it incorporates contradictory assumptions about what it is to argue objectively about norms. This gives rise to conflicting legal arguments and the inability to prefer any of them”.²⁷² (Matti Koskeniemi)

Tudo o que se disse na tese até o momento teve por objetivo inserir o leitor no pouco conhecido universo da inteligência de Estado, explicando suas formas de exercício e organização, tecendo algumas considerações sobre o contexto político que define a atuação da inteligência de alguns países e esboçando, com muitos exemplos, as capacidades operacionais de uma agência de inteligência nos dias atuais, associando-as aos principais problemas provocados por uma postura de coleta abrangente. Obviamente, toda essa extensa análise irá contribuir – para não dizer que foi imprescindível – para a discussão das hipóteses sobre as quais a tese se sustenta. Para tanto, agora compete-nos evoluir de uma análise puramente descritiva para um estudo dogmático de Direito Internacional, em que se pretende examinar possíveis parâmetros de licitude²⁷³ das atividades de espionagem – recordando que as atividades ordinárias de inteligência são perfeitamente lícitas de acordo com o Direito Internacional (cf. Introdução).

Mas falar em “licitude das atividades de espionagem segundo o Direito Internacional” ou perguntar “O Direito Internacional proíbe a espionagem?” é uma forma simplória de apresentar a questão. Há variáveis que podem qualificar uma atividade de espionagem segundo a natureza da informação envolvida, ou os titulares da informação, ou a finalidade da atividade, ou mesmo o modo como ela é realizada – tudo isso afetando a verificação de sua licitude. O próprio conceito que se tem de “espionagem” e a compreensão do que é a licitude no Direito Internacional irão influenciar na análise que ora se propõe.

²⁷¹ Grande parte do que se diz neste capítulo foi objeto de publicação anterior de minha autoria em: LIMA, Humberto Alves de Vasconcelos. Os Programas de Espionagem Cibernética em Massa e os Desafios à Proteção Internacional do Direito à Privacidade. In: POLIDO, Frabício Bertini Pasquot; ANJOS, Lucas Costa dos. [orgs.] **Marco Civil e Governança da Internet**: diálogos entre o doméstico e o global, Universidade Federal de Minas Gerais, pp. 443-471, 2016.

²⁷² KOSEKNNIEMI, M. **From Apology...** op. cit. p. 63.

²⁷³ Opta-se pelo vocábulo “licitude” significando contrariade ao ordenamento jurídico, em vez de “legalidade” que transmite melhor a ideia de “juridicidade”.

Se atentarmos para ao contexto em que a espionagem é praticada – se durante um conflito armado internacional ou em tempo de paz – alcançaremos um tipo de resposta para o problema. Se, por outro lado, focarmos na natureza da informação alvo da espionagem e nos seus titulares, podemos sugerir uma classificação tridimensional para a análise – espionagem de segredos de estado; espionagem de segredos de empresa e espionagem de informações privadas de particulares – como foi proposto no estudo do capítulo 3. Por fim, é possível ter por critério o meio através do qual a espionagem se realiza, se no espaço cibernético ou por imagens de satélites ou, de outro lado, por formas tradicionais que exijam intrusão territorial, como o envio de espiões ou sobrevoos clandestinos.

São muitas as complexidades, portanto, e é preciso sanar tais questões preliminares, estabelecendo critérios claros sobre o que se pretende discutir exatamente, para que então se possa avançar.²⁷⁴

4.1 A definição do conceito de espionagem

Há uma dificuldade em se definir “espionagem” para fins de estudo de Direito Internacional que se origina em razão de duas circunstâncias: a primeira é o fato de não haver qualquer documento que reflita um acordo entre Estados sobre o que é espionagem (ou mesmo “inteligência”), ou seja, não há um conceito formal de tais atividades estatais. O que há de mais próximo disso são as regras que regulamentam o tratamento do espião capturado no contexto de um conflito armado internacional (ver seção seguinte, 4.2), previstas no art. 46 do Protocolo I Adicional às Convenções de Genebra de 1949, relativo à proteção de vítimas. Lá há menção a “atividades de espionagem” e a definição do espião como sendo “O membro das forças armadas de uma Parte no conflito que recolha ou procure recolher, por conta dessa Parte, informações num território controlado por uma Parte adversa”.

A ausência de um conceito compreensivo de espionagem em um tratado ou outro documento regido pelo Direito Internacional não seria problema se não houvesse uma absoluta discrepância doutrinária sobre a definição da atividade, sendo esta a segunda circunstância que dificulta tal definição. De fato, autores divergem sensivelmente na tarefa de conceituar espionagem em trabalhos do

²⁷⁴ Algumas considerações que serão feitas a seguir já foram antecipadas nas seções II e III da Metodologia.

domínio do Direito Internacional. A. John Radsan²⁷⁵, Geoffrey B. Demarest²⁷⁶ e Manuel R. García-Mora²⁷⁷ adotaram um conceito restritivo de espionagem, definindo a atividade como a coleta clandestina de informações através de fontes humanas (HUMINT). “Espionagem é o que faz o espião”²⁷⁸, poderíamos assim resumir a ideia por trás do conceito acolhido por estes autores.

Outros autores mais atentos às diversas formas através das quais a inteligência clandestina pode ser praticada propõem conceitos que não se restringem à coleta por fontes humanas, resultando em definições mais abrangentes. Nesse sentido, David P. Fidler²⁷⁹ e M. Fabien Lafouasse²⁸⁰ constroem conceitos focados apenas no objetivo da espionagem, que é a coleta da informação sigilosa (elemento material) e na sua forma clandestina (elemento formal). Com efeito, para fins de estudos de Direito Internacional, essa abordagem é mais adequada pois tem o conveniente de englobar as diferentes formas de inteligência clandestina sob a mesma categoria, permitindo assim sua distinção em relação às atividades ordinárias de inteligência, essas últimas não gerando, a princípio, quaisquer preocupações relativas à sua licitude.

Dessa forma, recorda-se aqui o conceito de inteligência elaborado no capítulo 1 como sendo a atividade estatal através da qual são coletadas e analisadas

²⁷⁵ Como definido por A. John Radsan: “[...] *my focus is on the gathering of information from human beings through secret means. My definition of espionage, one of trench coats and Fedora hats, corresponds with the CIA’s self-pronounced status as the American master of espionage*”. RADSAN, A. John. The Unresolved Equation of Espionage and International Law. **Michigan Journal of International Law**, v. 28, 2007. p. 601.

²⁷⁶ Geoffrey B. Demarest afirma: “*Espionage, within its more specific, limited meaning, is human information collection*” e “[...] *espionage can be defined as the consciously deceitful collection of information, ordered by a government or organization hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the collecting*”. DEMAREST, Geoffrey B. Espionage in International Law. **Denver Journal of International Law and Policy**, v. 24, n. 2, 3, 1996. p. 323 e 325-326.

²⁷⁷ Segundo García-Mora, espionagem é “[...] *a clandestine activity, conducted in peace or in war, by a person commissioned by a foreign government for the purpose of obtaining secret information regarding another State’s national defense*”. GARCÍA-MORA, Manuel R. Treason, Sedition and Espionage as Political Offenses under the Law of Extradition. **University of Pittsburgh Law Review**, v. 26, 1964. p. 79.

²⁷⁸ Note-se que no idioma inglês há o termo genérico para espionagem, “*espionage*”, e o termo que designa a atividade do espião, “*spying*”. O que se faz segundo esse conceito é considerar sinônimos os dois termos.

²⁷⁹ “*Traditional espionage encompasses a government’s efforts to acquire clandestinely classified or otherwise protected information from a foreign government*”. FIDLER, David P. Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies. **ASIL Insights**, v. 17, n. 10, 2013. p. 1.

²⁸⁰ “*La recherche du renseignement se caractérise à la fois par son caractère clandestin et par les diverses méthodes employées à cette fin, qui ne se limitent plus à la seule utilisation de personnes physiques*”. LAFOUASSE, M. Fabien. Espionnage en droit international. **Annuaire français de droit international**, v. 47, 2001. p. 72.

informações de forma organizada e sistemática com a finalidade de orientar o processo decisório de suas autoridades. A espionagem, como operação clandestina de coleta de informação, é uma modalidade da inteligência. Pode ser tecnicamente definida como **a atividade de inteligência clandestina em que se objetiva coletar, através de uma operação sigilosa, informação classificada ou de outra forma mantida em segredo.**

É importante notar que o fato de ser a espionagem uma operação clandestina, isto é, oculta em relação ao Estado que dela é alvo e do público em geral, não significa que o Estado que a pratica se acautela de seu sigilo em claro reconhecimento de sua ilicitude. Seria um raciocínio semelhante ao apresentado pelo ex-vice-presidente dos Estados Unidos Al Gore, quando, ao aconselhar o Presidente Clinton em 1993 sobre um caso de “*extraordinary rendition*” – a captura de um terrorista em solo estrangeiro por agentes dos Estados Unidos e sua posterior entrega para interrogadores em um terceiro Estado, disse: “É claro que é uma violação do Direito Internacional; é por isso que é uma ação encoberta. O sujeito é um terrorista. Vá pegá-lo.”.²⁸¹ A conclusão pode fazer sentido se considerarmos operações tais como assassinatos dirigidos ou auxílios financeiros a ditadores, por exemplo, mas no caso da espionagem, o segredo da operação se justifica, como já observado anteriormente, pois, caso o detentor da informação identifique uma tentativa de coleta – por consequência frustrada – fará aumentar o rigor de sua proteção ou implantará informações falsas destinadas a enganar o coletor, reduzindo assim as chances de se obter a informação de que se precisa.

É preciso notar que esse conceito exclui de seu âmbito atividades que envolvam algum elemento de coerção, ainda que sejam conduzidas por agências de inteligência, como ocorre com outras operações encobertas, prática de tortura em interrogatórios e ataques cibernéticos. Logo, o conceito proposto lida com atividades não coercitivas de obtenção de informação.

Claramente delimitado o conceito de espionagem, seguem análises separadas de sua licitude segundo diferentes critérios.

²⁸¹ “Of course it’s a violation of international law, that’s why it’s a covert action”. The guy is a terrorist. Go grab his ass”. THE LONG, dark war. **The Economist**, 31 jul. 2008. Disponível em: <<http://www.economist.com/node/11837595>>

4.2 Os problemas de se posicionar a análise da licitude da espionagem sobre a dicotomia “guerra-paz”

Como já dito, existem diversos ângulos sob os quais o problema da licitude da espionagem internacional pode ser estudado. Uma forma de abordar o problema se dá de acordo com o contexto em que a atividade é realizada, se praticada durante um conflito armado internacional ou em tempo de paz.

Historicamente, em razão da inexistência de qualquer obrigação geral dos beligerantes de respeitar o território ou governo do Estado inimigo, como observou Quincy Wright²⁸², a espionagem realizada no contexto de um conflito armado internacional foi considerada lícita de acordo com o costume internacional²⁸³, posteriormente traduzido em regras convencionais. Os tratados que disciplinaram conflitos dessa natureza – como a Declaração de Bruxelas de 1874, as Convenções de Haia de 1899 e 1907 e as quatro Convenções de Genebra de 1949 e seus protocolos adicionais – dispuseram, de forma semelhante, que ao indivíduo flagrado em atividades de espionagem em território inimigo e que não esteja portando qualquer sinal distintivo de pertencer às tropas opostas (ex: uniforme), não será exigido concedê-lo o status de prisioneiro de guerra, podendo ele ser punido de acordo com as leis internas do Estado que o capturou. Isso inclui estar sujeito à pena de morte (Convenção IV de Genebra Relativa à Proteção de Civis em Tempo de Guerra, artigo 68), apesar de haver um dever do Estado que capturou o espião em submetê-lo a julgamento (Protocolo I Adicional às Convenções de Genebra de 1949, artigo 45 (3)). A execução sumária do espião capturado é vedada, portanto.

A regra vigente sobre o status do espião está prevista no artigo 46 do Protocolo I Adicional às Convenções de Genebra de 1949 relativo à Proteção das Vítimas dos Conflitos Armados Internacionais. Afirma-se em seu item 1:

²⁸² “*The legitimacy of espionage in time of war arises from the absence of any general obligation of belligerents to respect the territory or government of the enemy state, and from the lack of any specific convention against it*”. WRIGHT, Quincy. *Espionage and the Doctrine of Non-Intervention in Internal Affairs* in STANGER, Roland J. (Org.) **Essays on Espionage and International Law**, Ohio University Press, 1962. p. 12.

²⁸³ Em lição de Hugo Grócio: “*Spies, whose sending is beyond doubt permitted by the law of nations - such as the spies whom Moses sent out, or Joshua himself - if caught are usually treated most severely. "It is customary," says Appian, "to kill spies." Sometimes they are treated with justice by those who clearly have a just case for carrying on war; by others, however, they are dealt with in accordance with that impunity which the law of war accords. If any are to be found who refuse to make use of the help of spies, when it is offered to them, their refusal must be attributed to their loftiness of mind and confidence in their power to act openly, not to their view of what is just or unjust*”. GROTIUS, Hugo. **The Law of War and Peace**, 1625. Livro 3, capítulo 4, parágrafo XVIII.

[...] o membro das forças armadas de uma Parte no conflito que cair em poder de uma Parte adversa enquanto se dedica a atividades de espionagem não terá direito ao estatuto de prisioneiro de guerra e poderá ser tratado como espião.

A razão dessa disposição é evidente: não é razoável exigir de um Estado que teve suas informações clandestinamente obtidas que conceda o *status* de prisioneiro de guerra ao espião, pois a principal consequência dessa condição é a de que, no fim do conflito, deve o prisioneiro ser libertado (Convenção III de Genebra relativa ao Tratamento dos Prisioneiros de Guerra, art. 118). Dessa forma, as informações obtidas através da espionagem poderiam ser repassadas ao inimigo.

Por outro lado, o indivíduo que esteja realizando atividades de coleta de informações em território inimigo, mas enverga o uniforme de suas forças armadas – a “sentinela avançada” (*scout*) – deverá ser tratado como prisioneiro de guerra (art. 46, item 2 do Protocolo I), pois, ao contrário do espião que age clandestinamente, trata-se de um combatente identificável.

Diversamente, se um espião agindo clandestinamente em território inimigo, consegue retornar e se juntar às forças armadas à qual pertence, mas posteriormente é capturado, ele não poderá ser tratado como espião, devendo receber os privilégios do prisioneiro de guerra (art. 46, item 4 do Protocolo I). A lógica desta disposição parece residir no reconhecimento de que, nesse caso, retornando o espião, as informações por ele obtidas foram repassadas e não se justificaria, portanto, recusar-lhe o *status* de prisioneiro de guerra se capturado após o retorno. Como observa A. John Radsan, “um espião, portanto, tem um forte incentivo para ter sucesso em sua missão de espionagem e para retornar rapidamente para sua organização militar”.²⁸⁴

O evidente paradoxo do tratamento do espião nos conflitos internacionais, cujo envio tal como a captura e punição são considerados lícitos, segundo Simon Chesterman “reflete o limbo legal em que os espiões operam, um *status* intimamente relacionado à dúbia honra associada com atividades encobertas em geral”.²⁸⁵

A regulamentação da espionagem no contexto de um conflito armado leva o estudioso a procurar o mesmo tipo de disciplina para situações em que a atividade é

²⁸⁴ “A spy therefore has a strong incentive to succeed in his spying mission and to return quickly to his military organization”. RADSAN, J. A. *op. cit.* p. 602.

²⁸⁵ “[...] reflects the legal limbo in which spies operate, a status closely related to the dubious honor associated with covert activities generally”. CHESTERMAN, S. *op. cit.* p. 1078.

praticada em tempo de paz. Deparando-se ele com a inexistência de regras sobre a espionagem na ausência de beligerância internacional, automaticamente nota uma lacuna na dimensão positiva do Direito Internacional e constrói o problema da espionagem sobre a dicotomia guerra-paz. Autores que pensam a questão sobre esse ângulo normalmente abordam o fenômeno da “espionagem em tempo de paz” (*peacetime espionage*) de forma unitária, como se uma só atividade fosse, sem atenção aos diversos tipos de informação que pode ela objetivar ou os diferentes meios através dos quais pode se realizar.²⁸⁶

Essa abordagem tem um único mérito, que é o de não ignorar a existência de um regime normativo para atividades de espionagem no Direito Humanitário Internacional. Por outro lado, seu caráter reducionista simplifica a análise. Leva o estudioso a crer que toda forma de espionagem praticada em tempo de paz deve ser analisada como uma atividade única, cuja licitude poderia ser unitariamente verificada – ainda que se possa divergir na análise subsequente, que é a resposta sobre sua licitude, ou seja, se a atividade é ou não proibida pelo Direito Internacional. Pois, se se questiona nos seguintes e exatos termos: “A espionagem em tempo de paz é proibida pelo Direito Internacional?”, a única resposta adequada é um sonoro “depende”.

Não bastasse, a proposição de uma dicotomia guerra-paz soa maniqueísta nos dias atuais. A forma como muitos dos conflitos contemporâneos se manifestam – através de atores não estatais, muitas vezes na ausência de uma declaração formal de beligerância, alguns deles envolvendo ataques não físicos, como por exemplo os cibernéticos, ou direcionados, como bombardeamentos “cirúrgicos” com *drones* – situa-os numa zona cinzenta entre os dois contextos, outrora tão fáceis de distinguir. Já na década de 1960 a insuficiência dessa distinção dual foi notada por Richard Falk:

Um problema intelectual central surge quando se tenta pensar sobre o *status* da espionagem em categorias definidas pela tradicional dicotomia entre paz e guerra. A guerra fria e a revolução na tecnologia militar torna essa dicotomia inadequada como ferramenta

²⁸⁶ São muitos autores que analisam o problema da licitude da espionagem sobre a dicotomia Guerra-paz. Cf. PEYTON, Cooke. Bringing the Spies in from the Cold: Legal Cosmopolitanism and Intelligence Under the Laws of War. **University of San Francisco Law Review**, v. 44, 2010. p. 16; RADSAN, J. A. *op. cit.* p. 603; DEMAREST, G. B. *op. cit.* p. 330 ss. SCOTT, Roger D. Territorially Intrusive Intelligence Collection and International Law. **The Air Force Law Review**, 1999. p. 219 ss. e WRIGHT, Q. *op. cit.* p. 10.

de análise. Logo, o problema da espionagem no mundo contemporâneo desafia um analista jurídico a desenvolver um novo aparato conceitual que é capaz de lidar com o caráter transformado das relações internacionais.²⁸⁷

Aceitando o desafio de Richard Falk, propõe-se na tese uma nova forma de pensar o problema da licitude da espionagem internacional, substituindo o *critério geopolítico* “guerra-paz” por um *critério material*, que distingue diferentes atividades de espionagem de acordo com a natureza do titular e da própria informação coletada ou que se pretenda coletar. Orientando-se por esse critério, sugere-se analisar a licitude das atividades de espionagem segundo uma visão tridimensional, focada na espionagem de informações privadas de particulares, segredos de empresa e segredos de Estado.²⁸⁸ Essa abordagem é inspirada pelo reconhecimento de que o Direito Internacional possui diferentes regimes normativos para a proteção do sigilo de informações que restringem a prática da espionagem de forma indireta, sendo que a verificação taxativa feita por muitos autores de que a espionagem em tempo de paz não é regulamentada no Direito Internacional²⁸⁹ merece ser analisada com cuidado. De fato, o aparente silêncio do Direito Internacional sobre as atividades de espionagem fora do contexto do Direito Humanitário parece ser muito mais resultado de uma escolha latente e comum de política internacional dos Estados do que uma lacuna, no sentido de falha ou regulamentação deficiente do tópico. Como observou Simon Chesterman, “inteligência é menos uma lacuna na ordem jurídica do que é o elefante na sala”.²⁹⁰

²⁸⁷ “A central intellectual problem arises when one tries to think about the status of espionage in the categories set by the traditional dichotomy between peace and war. The cold war and the revolution in military technology make this dichotomy inadequate as a tool of analysis. Thus the problem of espionage in the contemporary world challenges a legal analyst to develop a new conceptual apparatus that is able to cope with the transformed character of international relations”. FALK, Richard. Foreword in STANGER, R. J. *op. cit.* p. viii.

²⁸⁸ Zahra Baheri e Ali Shojaei Fard propõem algo semelhante quando estratificam a espionagem em: espionagem militar, espionagem econômica, espionagem de fontes ambientais e espionagem política. Cf. BAHERI, Zahra; FARD, Ali Shojaei. Status of espionage from the perspective of international laws with emphasis on countries' diplomatic and consular relations. **Journal of Scientific Research and Development**, v. 2, n. 1, 2015. p. 42.

²⁸⁹ “International law regarding peacetime espionage is virtually unstated, and thus, international law has been an inappropriate and inadequate reference for either condemnation or justification of actions involving intelligence gathering” DEMAREST, G. B. *op. cit.* p. 321; “No international convention has ever addressed the legality of peacetime espionage”. SCOTT, R. D. *op. cit.* p. 218. “Fundamentally, peacetime regulation of intelligence activities has always and consistently been held to be within the sole province of domestic law”. SULMASY, Glenn; YOO, John. Counterintuitive: Intelligence Operations and International Law. **Michigan Journal of International Law**, v. 28, 2006-2007. p. 627.

²⁹⁰ “Intelligence is less a lacuna in the legal order than it is the elephant in the room”. CHESTERMAN, S. *op. cit.* p. 1072.

4.3 A discussão sobre a licitude da espionagem de informações privadas de particulares

Ainda que seja verdadeiro o fato de não haver proibição expressa às atividades de espionagem no Direito Internacional, há algumas situações em que o segredo da informação é por ele tutelado e, por consequência, a obtenção dessa informação em circunstâncias não previstas no tratado que a protege seria considerada ilícita. Em outros termos, pode-se dizer que, nesses casos, a espionagem seria proscrita pelo Direito Internacional de forma reflexa. É exatamente isso o que acontece com as informações privadas de particulares, protegidas no Direito Internacional através da tutela do direito humano à privacidade.

4.3.1 A proteção internacional do direito humano à privacidade

O processo de internacionalização dos direitos humanos, que tem como marco inicial o fim da segunda guerra mundial, sempre teve incluída a proteção da privacidade em sua agenda. O art. XII da Declaração Universal dos Direitos Humanos (1948) – o primeiro documento que compreende um compromisso²⁹¹ de proteção internacional a essa categoria de direitos – já dispunha que “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.” O art. 17 do Pacto Internacional de Direitos Civis e Políticos (1966)²⁹², o art. 11(2) da Convenção Americana de Direitos Humanos²⁹³ e o art. 8(1) da Convenção Europeia de Direitos

²⁹¹ Uma noção muito clara subjacente à assinatura da Declaração era a de que não estavam os Estados-Signatários diante de um tratado ou outra espécie de acordo com força vinculante ou cogente (*binding force*). Originalmente, seria a Declaração melhor enquadrada na categoria de *soft law* – aqueles documentos que contêm compromissos cujas violações a princípio não implicam qualquer consequência jurídica para o Estado violador, muito embora possam, ao longo do tempo, se integrar à prática estatal e eventualmente formar costume internacional. Com efeito, reconhece-se que a Declaração Universal dos Direitos Humanos adquiriu, através desse processo, *status* de costume internacional e, portanto, seus enunciados são obrigações vinculantes de Direito Internacional. Cf. SCHUTTER, Olivier De. **International Human Rights Law**, Cambridge University Press, 2010. p. 50.

²⁹² “1. Ninguém será objeto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e reputação. 2. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques”.

²⁹³ “2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação”.

Humanos²⁹⁴ – todos compromissos dotados de força cogente – trazem disposições semelhantes.

É importante ressaltar que, ao elencarem a privacidade à categoria de direito humano, os Estados reconhecem sua superioridade axiológica e a posicionam, juntamente com as demais espécies de direitos humanos, em um patamar hierarquicamente superior às obrigações de outra natureza. Com efeito, a Carta da Organização das Nações Unidas, em seu art. 1(3), exalta o “respeito aos direitos humanos e às liberdades fundamentais” como um de seus propósitos centrais. Na medida em que o art. 103 da Carta determina que as obrigações nela assumidas devem prevalecer caso conflitem com obrigações contraídas em outro acordo internacional, conclui-se que o dever de proteger direitos humanos tem natureza prioritária.²⁹⁵

A proteção dos direitos humanos no Direito Internacional opera sobre um sistema bastante peculiar. Em primeiro lugar nota-se que os tratados de direitos humanos normalmente não vinculam aos Estados obrigações a serem adimplidas além dos limites de sua “jurisdição”.²⁹⁶ Ao ratificar um tratado dessa natureza, um Estado se vê obrigado a proteger direitos humanos de pessoas que se encontram sob seu “controle efetivo”²⁹⁷ – esse o real sentido da expressão “jurisdição” –

²⁹⁴ “1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência”.

²⁹⁵ A questão da hierarquia da proteção dos direitos humanos sobre outras obrigações é controversa na doutrina jusinternacionalista. A prevalência das obrigações assumidas na Carta da ONU é um dos argumentos concordantes com a superioridade hierárquica dos direitos humanos. Outro argumento sustenta-se na ideia de que algumas espécies de direitos humanos adquiriram o *status* de *jus cogens* (e.g.: proibição do *non-refoulement* – proibição de fazer retornar a pessoa para o Estado do qual ela se retirou caso haja risco para sua vida ou integridade física e psicológica). Cf. SCHUTTER, O. D. *op. cit.* p. 60-65.

²⁹⁶ O Pacto Internacional de Direitos Civis e Políticos determina, em seu art. 2(1), que: “Cada um dos Estados-Signatários no presente pacto compromete-se a respeitar e a garantir a todos os indivíduos que se encontrem no seu **território** e estejam sujeitos à sua **jurisdição**, os direitos reconhecidos no presente pacto, sem distinção alguma de raça, cor, sexo, idioma, religião, opiniões políticas ou de outra natureza, origem nacional ou social, posição econômica, nascimento ou qualquer outra condição social”. Já a Convenção Europeia de Direitos Humanos e a Convenção Americana de Direitos Humanos, ambas em seu art. 1, suprimiram a expressão “território”, satisfazendo-se com a “jurisdição” do Estado sobre o indivíduo. Confira-se o texto da Convenção Europeia: “As Altas Partes Contratantes reconhecem a qualquer pessoa dependente da sua **jurisdição** os direitos e liberdades definidos no título I da presente Convenção”. Já a Carta Africana de Direitos Humanos não faz menção nem a “território” nem a “jurisdição”, afirmando em seu art. 2 que “Toda a pessoa tem direito ao gozo dos direitos e liberdades reconhecidos e garantidos na presente Carta...”. [g.n.]

²⁹⁷ “The ‘jurisdiction’ of a State may extend beyond its national territory, where that State exercises effective control, for instance following a military invasion, of other portions of territory. It should not matter whether such occupation is, under international law, legal or illegal”. SCHUTTER, O. D. *op. cit.* p. 125. O *leading case* sobre a compreensão da “jurisdição” como “controle efetivo” foi a decisão do Comitê de Direitos Humanos no caso *López Burgos v. Uruguay* (1979), que dizia

estejam elas em seu território ou não, sejam elas nacionais ou estrangeiros. Como consequência, pode-se afirmar que os Estados não estão obrigados a proteger direitos humanos em situações que escapam à sua “jurisdição”.

Em segundo lugar é importante notar o caráter objetivo dos direitos humanos, no sentido de que “não são redutíveis a trocas bilaterais de vantagens entre os Estados contratantes”.²⁹⁸ Isto é, os tratados de direitos humanos não possuem natureza contratual e portanto não se realizam sob a lógica da bilateralidade. Um Estado não pode – ou não faz sentido que ele o faça – “retaliar” ou “protestar” violações de direitos humanos por parte de outros Estados violando ele próprio direitos humanos de seus cidadãos.

As decisões e pareceres de cortes e outros órgãos de proteção e fiscalização dos direitos humanos acerca do direito à privacidade e as atividades de inteligência estatal formam um conjunto significativo. O Parlamento Europeu – um órgão de natureza política – ao apreciar a existência do ECHELON, o sistema global de interceptação de comunicações transmitidas via satélites (v. seção 1.2.2, “b” – Inteligência de Sinais), ressaltou os riscos que atividades de vigilância impõem sobre a privacidade individual:

Qualquer ato envolvendo interceptação de comunicações, e mesmo a gravação de dados por serviços de inteligência para esse propósito, representa uma séria violação da privacidade de um indivíduo. Somente em um “Estado policial” a interceptação irrestrita de comunicações é permitida por autoridades do governo. Em contraste, nos Estados membros da União Europeia, que são democracias maduras, a necessidade de órgãos do Estado – e, portanto, também dos serviços de inteligência – de respeitar a privacidade individual é inquestionável e é geralmente consagrada em constituições nacionais. A privacidade, então, goza de especial proteção: violações potenciais são autorizadas somente após a

respeito ao sequestro de um cidadão uruguaio em exílio em solo argentino pela inteligência do Uruguai, que foi seguidamente torturado após sua captura. Já a Corte Internacional de Justiça, no parecer sobre As Consequências Jurídicas da Construção de um Muro nos Territórios Palestinos Ocupados (2004), apresentou o mesmo entendimento quando afirmou: “*The Court would observe that, while the jurisdiction of States is primarily territorial, it may sometimes be exercised outside the national territory. Considering the object and purpose of the International Covenant on Civil and Political Rights, it would seem natural that, even when such is the case, States parties to the Covenant should be bound to comply with its provisions [...]* The travaux préparatoires of the Covenant confirm the Committee’s interpretation of Article 2 of that instrument. These show that, in adopting the wording chosen, the drafters of the Covenant did not intend to allow States to escape from their obligations when they exercise jurisdiction outside their national territory. They only intended to prevent persons residing abroad from asserting, vis-à-vis their State of origin, rights that do not fall within the competence of that State, but of that of the State of residence”.

²⁹⁸ “Human rights treaties have an ‘objective’ character in that they are not reducible to bilateral exchanges of advantages between the contracting States”. SCHUTTER, O. D. op. cit. p. 94.

análise das considerações jurídicas e de acordo com o princípio da proporcionalidade.²⁹⁹

No âmbito da ONU, importantes discussões sobre o direito à privacidade já foram travadas. O Comitê de Direitos Humanos – órgão da ONU responsável pelo monitoramento do cumprimento dos Pactos Internacionais de 1966 – já se pronunciou no sentido de serem as atividades de vigilância incompatíveis com a proteção do direito à privacidade:

Vigilância, seja eletrônica ou de outra forma, interceptações de comunicações telefônicas, telegráficas e outras formas de comunicação, escutas e gravação de comunicações devem ser proibidas.³⁰⁰

A esse respeito, um importante documento é a resolução 68/167 da Assembleia Geral da ONU, intitulado “O Direito à Privacidade na Era Digital”, em que, reafirmando o direito fundamental à privacidade e expressando preocupação com o impacto negativo que a vigilância em massa pode ter no exercício e gozo dos direitos humanos, se convoca a comunidade internacional a adotar medidas eficazes à proteção desse direito no contexto das comunicações digitais.³⁰¹

Nesse sentido, iniciativas relevantes para o debate acerca dos desafios da proteção da privacidade diante de programas de vigilância em massa estão sendo conduzidas no Conselho de Direitos Humanos da ONU. O Relator Especial para a “Promoção e Proteção dos Direitos Humanos e Liberdades Individuais durante o Combate ao Terrorismo”, Ben Emmerson, fez importantes contribuições nesse sentido. O Relator reconheceu que a privacidade pode ser limitada legitimamente para atividades de persecução penal e contraterrorismo quando o indivíduo esteja

²⁹⁹ “Any act involving the interception of communications, and even the recording of data by intelligence services for that purpose, represents a serious violation of an individual’s privacy. Only in a ‘police state’ is the unrestricted interception of communications permitted by government authorities. In contrast, in the EU Member States, which are mature democracies, the need for state bodies, and thus also intelligence services, to respect individuals’ privacy is unchallenged and is generally enshrined in national constitutions. Privacy thus enjoys special protection: potential violations are authorised only following analysis of the legal considerations and in accordance with the principle of proportionality”. EUROPEAN UNION. European Parliament. **Report...** *op. cit.* p. 83.

³⁰⁰ “Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited”. UNITED NATIONS. The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art. 17), **Human Rights Committee**, General Comment nº 16, item 8, 8 abr. 1988.

³⁰¹ UNITED NATIONS GENERAL ASSEMBLY. **The right to privacy in the digital age**. Resolution 68/167, 21 jan. 2014. Disponível em: <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>

sujeito a uma investigação formal em curso. Todavia, a própria existência de programas de vigilância em massa foi considerada pelo Relator como uma “interferência potencialmente desproporcional” ao direito à privacidade. Observou o Relator ainda que o respeito ao princípio geral segundo o qual o Estado deve se valer do meio menos intrusivo possível para interferir na privacidade individual só poderia ocorrer numa análise caso-a-caso.³⁰²

O Conselho também determinou em 24 de março de 2015 que o Alto Comissariado da ONU para os Direitos Humanos instituísse o cargo de Relator Especial Sobre o Direito à Privacidade, com um mandato de três anos.³⁰³ As conclusões do Relator, Joseph Cannataci, serão apresentadas após a conclusão desta tese, mas já se demonstrou especial preocupação com os programas de vigilância em massa no domínio cibernético e a política anti-criptografia adotada por alguns governos.³⁰⁴

Nas cortes regionais de proteção aos direitos humanos, o direito à privacidade tem recebido tutela tão efetiva quanto a de qualquer outra espécie de direito. A experiência da Corte Europeia de Direitos Humanos nessa tarefa tem relevância particular em razão dos desafios de interpretação impostos pela “cláusula de interferência” no direito à privacidade prevista no art. 8(2) da Convenção Europeia de Direitos Humanos – que não encontra correspondente nos outros tratados de proteção aos direitos humanos. O dispositivo determina que ingerências da autoridade pública no exercício do direito à privacidade somente serão permitidas se: a) previstas em lei e (1) consistirem em medida necessária para a segurança nacional, (2) para a segurança pública, (3) para o bem-estar econômico do país, (4) a defesa da ordem e a prevenção das infrações penais, (5) a proteção da saúde ou da moral, (6) **ou** a proteção dos direitos e das liberdades de terceiros. Há, portanto, um requisito obrigatório, que é a previsão legal da medida de interferência, que deve ser cumulado alternativamente com ao menos um dos seis outros requisitos.

³⁰² UNITED NATIONS GENERAL ASSEMBLY. **Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.** A/69/397, 23 set. 2014. §§ 18 e 30. Disponível em <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/pdf/N1454519.pdf?OpenElement>>

³⁰³ UNITED NATIONS GENERAL ASSEMBLY. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. **Human Rights Council**, Resolution 28/16, 24 mar 2015. Disponível em: <http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/28/L.27>

³⁰⁴ UNITED NATIONS GENERAL ASSEMBLY. Report of the Special Rapporteur on the right to privacy. A/HRC/31/64, **Human Rights Council**. 8 mar. 2016. Disponível em: <<http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>>

O texto do art. 8(2) da Carta Europeia parece demasiadamente amplo e vago de forma a possibilitar que qualquer ato estatal possa ser enquadrado em alguma das hipóteses de limitação da privacidade – obviamente, desde que a medida esteja autorizada em lei, como resguarda o texto da Convenção. As dificuldades enfrentadas pela Corte Europeia de Direitos Humanos no que diz respeito à aplicação do direito à privacidade, dessa forma, se concentra na busca por um adequado equilíbrio entre privacidade individual e outros valores igualmente importantes à coletividade.

De forma geral, o princípio do art. 8 protege informação pessoal sobre a qual o indivíduo tem uma expectativa legítima de não ser publicada sem seu consentimento (*Flinkkilä and Others v. Finland*, processo nº 25576/04, § 75, julgamento em 6 abr. 2010).³⁰⁵ Em relação às atividades de vigilância em especial, a Corte Europeia observou, no caso *Klass and Others v. Germany* – em que se apreciava legislação do país que autorizava a monitoração de correspondências e ligações telefônicas sem que fosse necessário informar posteriormente os indivíduos monitorados das medidas que contra eles foram adotadas – que a cláusula de interferência do art. 8(2) da Carta deve ser interpretada de forma restritiva, a exigir que a vigilância secreta sobre cidadãos somente seja tolerada na medida em que for necessária para a salvaguarda das instituições democráticas. Além disso, considerando que, enquanto secreta, a vigilância escapa ao controle judicial, a Corte julgou ser necessária a notificação do indivíduo monitorado uma vez terminada as interceptações, desde que tal procedimento não colocasse em risco a segurança nacional ou o próprio propósito da operação de inteligência.³⁰⁶

No mesmo sentido, no importante julgado *Rotaru v. Romania*, a Corte Europeia asseverou que as atividades de vigilância devem observar os princípios de uma sociedade democrática e do Estado de Direito, e serem supervisionadas pelo judiciário que possui melhores condições de garantir imparcialidade, independência e o devido processo legal.

³⁰⁵ EUROPEAN COURT OF HUMAN RIGHTS. **Internet: case-law of the European Court of Human Rights**, jun 2015. Disponível em: <http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf>

³⁰⁶ “This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions”. EUROPEAN COURT OF HUMAN RIGHTS. **Klass and Others v. Germany**, Processo nº 5029/71, julgamento em 6 set. 1978.

A Corte também deve estar satisfeita com a existência de salvaguardas adequadas e eficazes contra o abuso, uma vez que um sistema de vigilância secreta projetado para proteger a segurança nacional implica o risco de minar ou mesmo destruir a democracia com o pretexto de defendê-la [...] Para que os sistemas de vigilância secreta sejam compatíveis com o artigo 8 da Convenção, devem conter salvaguardas estabelecidas por lei que se apliquem à supervisão das atividades dos serviços relevantes. Procedimentos de supervisão devem seguir os valores de uma sociedade democrática o mais fielmente possível, em particular, do Estado de Direito, o que é expressamente referido no preâmbulo da Convenção. O Estado de Direito implica, entre outras coisas, que a interferência das autoridades do executivo nos direitos individuais devem ser sujeitas a uma supervisão eficaz, que normalmente deve ser realizada pelo Poder Judiciário, pelo menos em última instância, uma vez que o controle judicial oferece as melhores garantias de independência, imparcialidade e de um procedimento adequado.³⁰⁷

Em outros casos a condenação do Estado por violação ao Direito à Privacidade em situações de vigilância ocorreu em razão da falta de clareza da lei sobre os limites do exercício discricionário que possuem as autoridades na condução desse tipo de atividade (*Kruslin v. France*, n. 11801/85, 24 abr. 1990; *Kopp v. Switzerland*, n. 13/1997/797/1000, 25 mar. 1998; *Amann v. Switzerland*, n. 27798/95, 16 fev. 2000; *Dragojević v. Croatia*, n. 68955/11, 15 jan. 2015).

A Corte Europeia também já teve a oportunidade de decidir sobre a licitude de programas de vigilância em massa. No caso *Roman Zakharov v. Russia*, a condenação do Estado por violação ao direito de privacidade se deu em decorrência do seu sistema de interceptação secreta de comunicações de telefonia celular. A legislação russa questionada compelia operadoras de telefonia celular a instalar equipamentos que permitiam o acesso direto do Serviço de Segurança Federal (*Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii – FSB*) às comunicações, sem necessidade de prévia autorização judicial. Foram observadas fragilidades na legislação no que diz respeito às circunstâncias em que as autoridades públicas

³⁰⁷ “The Court must also be satisfied that there exist adequate and effective safeguards against abuse, since a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it [...] In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services’ activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual’s rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure”. EUROPEAN COURT OF HUMAN RIGHTS. **Rotaru v. Romania**, Processo nº 28341/95, julgamento em 4 maio 2000.

poderiam se valer de medidas de vigilância secreta; a duração de tais medidas e as situações em que deveriam elas cessar; os procedimentos e regras sobre a supervisão das interceptações e o armazenamento e destruição dos dados e, principalmente, a inefetividade dos remédios disponíveis para questionar judicialmente as interceptações.³⁰⁸

No caso *Szabó and Vissy v. Hungary*, a legislação antiterrorista da Hungria foi questionada por não oferecer garantias legais contra o abuso, a permitir medidas desproporcionais e injustificáveis de limitação ao direito à privacidade. Notou-se que tais medidas de vigilância eram conduzidas quase que inteiramente na esfera do executivo e possibilitavam que virtualmente qualquer cidadão húngaro fosse alvo de interceptação de comunicações. A Corte considerou que qualquer medida de interferência, ainda que potencial, na privacidade dos cidadãos através de tecnologias inovadoras de vigilância somente pode ser realizada se for “necessária em uma sociedade democrática”, o que significa dizer:

[...] o requisito “necessária em uma sociedade democrática” deve ser interpretado nesse contexto como a exigir “estrita necessidade” em dois aspectos. Uma medida de vigilância secreta pode ser considerada de acordo com a Convenção apenas se for estritamente necessária, sob uma consideração geral, à salvaguarda de instituições democráticas e, além disso, sob uma consideração particular, para a obtenção de informação vital em uma operação individual. Na visão da Corte, qualquer medida de vigilância secreta que não corresponda a esses critérios estará sujeita ao abuso de autoridades com tecnologias formidáveis à sua disposição.³⁰⁹

Três outros importantes casos, ainda pendentes de julgamento, são *10 Human Rights Organisations and Others v. the United Kingdom; Big Brother Watch and Others v. the United Kingdom* (nº 58170/13) e *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* (nº 62322/14), todos questionando, em reação

³⁰⁸ EUROPEAN COURT OF HUMAN RIGHTS. **Roman Zakharov v. Russia**, Processo nº 47143/06, julgamento em 4 dez. 2015.

³⁰⁹ “[...] the requirement ‘necessary in a democratic society’ must be interpreted in this context as requiring ‘strict necessity’ in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court’s view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal”. EUROPEAN COURT OF HUMAN RIGHTS. **Szabó and Vissy v. Hungary**. Processo nº 37138/14, julgamento em 12 jan. 2016.

às revelações de Edward Snowden, os programas de vigilância em massa conduzidos pela agência de inteligência de sinais britânica GCHQ e pela NSA.

Já a experiência da Corte Interamericana de Direitos Humanos na proteção do direito à privacidade perante atividades de vigilância poderia ser mais profícua caso os Estados Unidos houvessem ratificado a Convenção Americana de Direitos Humanos, o que infelizmente não ocorreu. No caso *Escher e outros v. Brasil*, a Corte se pronunciou sobre a compatibilidade de atividades de escutas telefônicas com o direito à privacidade. Segundo a Corte, a proteção à privacidade nesse contexto é manifestada pelo direito de que o conteúdo da conversa e outros aspectos inerentes ao processo de comunicação (os metadados: o destino e origem das ligações, a identidade dos interlocutores e a frequência e duração da conversa, por exemplo) não sejam ilegalmente obtidos por terceiros – ressalvadas interferências legítimas estabelecidas por lei e que persigam uma finalidade legítima e necessária em uma sociedade democrática.³¹⁰

Em resumo, pode-se dizer que as decisões e outras formas de manifestação de cortes e órgãos internacionais de proteção aos direitos humanos sobre a tutela da privacidade diante de atos de vigilância estatal formam um conjunto de enunciados coerentes. Como uma *cláusula interpretativa geral*, considera-se que as atividades de vigilância estatal somente são legítimas caso **a)** estritamente necessárias à defesa de instituições democráticas. De fato, esse requisito visa reduzir à ilicitude qualquer atividade de inteligência que sirva a propósitos ditatoriais, em Estados-Policiais de que a história, especialmente europeia, está recheada de exemplos. Em adição, há a *cláusula legal* que exige a **b)** previsão da medida de vigilância em lei. Esta lei deve conter o atributo conhecido como “qualidade da lei”³¹¹, o que significa especificar **i)** as circunstâncias em que os serviços de inteligência e segurança podem realizar atividades de vigilância; **ii)** a duração de tais medidas; **iii)** as situações em que devem elas cessar; **iv)** os procedimentos e regras sobre a

³¹⁰ “In brief, the protection of privacy is manifested in the right that individuals other than those conversing may not illegally obtain information on the content of the telephone conversations or other aspects inherent in the communication process [...] Nevertheless, as Article 11(2) of the Convention makes clear, the right to privacy is not an absolute right and can be restricted by the States, provided interference is not abusive or arbitrary; to this end, it must be established by law, pursue a legitimate purpose and be necessary in a democratic society.” INTER-AMERICAN COURT OF HUMAN RIGHTS. **Case of Escher et al. v. Brazil**, julgamento em 6 jul. 2009. p. 32.

³¹¹ Sobre o requisito “quality of law”, cf. UNITED NATIONS GENERAL ASSEMBLY. **Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism**. *op. cit.* § 35.

supervisão das interceptações e o armazenamento e destruição dos dados e **v)** os remédios disponíveis para questionar judicialmente as interceptações. **c)** A supervisão das atividades de vigilância pelo Poder Judiciário é considerada o mecanismo que oferece as melhores garantias de independência, imparcialidade e de um procedimento adequado. Ela deve ser feita tanto previamente à realização da vigilância, através de uma ordem judicial que autorize a medida “caso a caso”, quanto posteriormente, por meio de uma ação judicial. Para que esse controle posterior seja possível, considera-se necessária **d)** a notificação do indivíduo uma vez cessada a vigilância a que ele foi submetido, desde que tal medida não implique em risco para a segurança nacional ou não comprometa a própria finalidade da operação de inteligência.

Como se nota, diante desses requisitos as atividades de vigilância em massa se tornam impraticáveis, podendo-se concluir então que a jurisprudência referente à proteção internacional do direito humano à privacidade sinaliza uma proibição a esse tipo de operação. Não é possível, por razões práticas, sujeitar a massiva quantidade de intervenções na privacidade de cidadãos a um rigoroso controle judicial de análise da licitude de cada uma delas, no qual sejam examinadas sua finalidade, proporcionalidade e estabelecidos limites tais como a duração da vigilância e quais informações podem ser armazenadas.

Mas recorde-se que os tratados de proteção aos direitos humanos vinculam aos Estados obrigações referentes às pessoas que estão sob sua jurisdição, entendida como controle efetivo sobre o indivíduo. Ora, nessas condições, o que dizer a respeito da vigilância feita sobre pessoas que escapam ao controle do Estado? De fato, a vigilância em massa conduzida por agências de inteligência também tem por alvo pessoas que se encontram em solo estrangeiro e não estão sob controle do Estado que patrocina a operação. Seria também ilícita a vigilância em massa nesse caso de acordo com a jurisprudência relativa à proteção internacional da privacidade que tem se construído até o momento?

A legislação interna dos países que compõem o grupo *Five Eyes* adotam regimes assimétricos de proteção quando discriminam a vigilância dirigida contra nacionais e residentes permanentes de um lado e, de outro, a que tem por alvo estrangeiros e pessoas que se encontram fora do território nacional. O *FISA (Foreign Intelligence Surveillance Act)* dos Estados Unidos – cujo próprio nome já indica um tratamento díspar do estrangeiro – restringe a realização da espionagem doméstica

a circunstância excepcionalíssimas, inclusive especificando medidas de destruição da informação obtida acidentalmente de comunicações em que tanto o remetente quanto o destinatário se encontram em solo estadunidense.³¹² O *Intelligence Service Act* de 2001 da Austrália, o *Government Communications Security Bureau Act* de 2003 da Nova Zelândia, o *National Defense Act* do Canadá e o *Regulation of Investigatory Powers Act* de 2000 do Reino Unido fazem discriminações em linhas semelhantes de nacionalidade ou extraterritorialidade.³¹³

Todavia, no contexto da proteção internacional dos direitos humanos, um tratamento díspar de um cidadão nacional ou residente permanente frente a um estrangeiro não residente é incoerente com outros princípios que informam o sistema de proteção como um todo. Se é certo, como já dito, que há uma obrigação do Estado de garantia dos direitos humanos de pessoas que se encontram sob sua jurisdição – pois de outra forma o Estado não disporia de meios jurídicos e práticos para sua proteção – pode-se afirmar também com segurança que o princípio da igualdade e da não-discriminação fazem com que exista ao menos um dever de abstenção de violação dos direitos humanos das pessoas que escapam à sua jurisdição. Outra não pode ser a conclusão que se alcança após a leitura do art. 26 do Pacto Internacional de Direitos Civis e Políticos:

Todas as pessoas são iguais perante a lei e têm direito, sem discriminação alguma, a igual proteção da Lei. A este respeito, a lei deverá proibir qualquer forma de discriminação e garantir a todas as pessoas proteção igual e eficaz contra qualquer discriminação por motivo de raça, cor, sexo, língua, religião, opinião política ou de outra natureza, origem nacional ou social, situação econômica, nascimento ou qualquer outra situação.

Pode-se afirmar, portanto, que o art. 17 do Pacto (Proteção da Privacidade) deve ser lido em consonância com o art. 26 (Igualdade e não-discriminação).³¹⁴

É verdade que em outros domínios alheios à proteção dos direitos humanos um Estado pode legitimamente impor discriminações legais em favor de seus

³¹² UNITED STATES OF AMERICA. *Foreign...* op. cit, § 1806 (i). Disponível em: <<https://www.law.cornell.edu/uscode/text/50/1806>>

³¹³ UNITED NATIONS GENERAL ASSEMBLY. **The right to privacy in the digital age**: Report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/27/37, 30 jun. 2014. p. 12, nota de rodapé nº 30. Disponível em: <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/088/54/pdf/G1408854.pdf?OpenElement>>

³¹⁴ UNITED NATIONS GENERAL ASSEMBLY. **The right to privacy in the digital age**: Report... op. cit. p. 12, § 36.

próprios cidadãos, especialmente quando justificadas em razão da segurança nacional. Um bom exemplo são as limitações de ocupação de cargos oficiais de alta relevância a nacionais, como o de Presidente, Ministro das Relações Exteriores e Chefe das Forças Armadas, que se verificam em diversos países. Entretanto, situação diversa é a violação deliberada de direitos de estrangeiros. Nas palavras de Ronald Dworkin:

[...] uma nação pode – e em algum grau deve – discriminar em favor de seus próprios cidadãos e, por consequência, contra aqueles que não o são. Mas a inflicção deliberada de dano é diferente, e o governo não tem direito ou autoridade de deliberadamente lesar estrangeiros por razões ou em circunstâncias nas quais não seria permitido lesar seus próprios cidadãos. [...] No domínio dos direitos humanos não há lugar para passaportes.³¹⁵

Além disso, como observa Marko Milanovic, se a razão de se proteger a privacidade é o valor da autonomia e da independência dos indivíduos a permitir que conduzam suas vidas sem a intrusão do Estado, então distinções baseadas apenas no critério da nacionalidade são difíceis de se justificar. Isso porque, não se pode sustentar racionalmente que não-cidadãos, como uma classe de pessoas, são essencialmente mais perigosos à segurança de um Estado do que seus próprios cidadãos, notadamente quando se observa que muitos dos atentados terroristas são praticados por nacionais ou residentes permanentes³¹⁶ (ex: os atentados no metrô de Londres em 2005, as explosões na maratona de Boston em 2013, os atentados de Paris de 2015 e o massacre na boate *Pulse* em Orlando, em 2016).

Uma outra forma de se encarar o problema é considerar que o controle exigido pelo requisito da “jurisdição” em casos de vigilância extraterritorial diz respeito à informação, não ao titular dela. Dessa forma, um Estado que detém acesso à informação, tenha sido ele obtido clandestinamente ou não, é aquele que

³¹⁵ “[...] a nation may—and to some degree must—discriminate in favor of its own citizens and therefore against those not its own. But the deliberate infliction of injury is different, and government has no right or authority deliberately to injure foreigners for reasons or in circumstances in which it would not be permitted to injure its own citizens. [...] The domain of human rights has no place for passports”. DWORKIN, Ronald. **Is Democracy Possible Here?: principles for a new political debate**. Princeton University Press, 2006. p. 48.

³¹⁶ “If the rationale for protecting privacy interests is the value of the autonomy and independence of individuals-of enabling them to lead their lives without state intrusion-then distinctions based on nationality alone would seem hard to justify. This is particularly so because it simply cannot reasonably be argued that non-citizens as a class are inherently more dangerous to the security of a state than its own citizens or permanent residents”. MILANOVIC, Marko. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. **Harvard International Law Journal**, v. 56, n. 1, 2015. p. 99.

efetivamente tem o domínio sobre a privacidade do indivíduo no que toca especificamente a esta informação. Essa interpretação foi endossada pelo Alto Comissariado da ONU para os Direitos Humanos:

[...] vigilância digital, portanto, pode fazer surgir obrigações de direitos humanos se envolver o exercício de poder ou controle efetivo de um Estado sobre infraestruturas de comunicação digital, onde quer que se encontrem, por exemplo, por meio de escutas diretas ou a penetração dessa infraestrutura. Da mesma forma, quando o Estado exerce jurisdição regulatória sobre um terceiro que controla fisicamente os dados, o Estado também teria obrigações decorrentes do Pacto [internacional de direitos civis e políticos].³¹⁷

Por fim, um outro problema que preocupa na proteção da privacidade diante de atividades de vigilância diz respeito às redes de compartilhamento de informação, tal como os *Five Eyes*. Na ausência de regras internacionais que disciplinem a colaboração entre serviços de inteligência, os Estados estão livres para ajustar tratados secretos de compartilhamento de informação que não estão sujeitos à supervisão de qualquer autoridade independente. Assim, um Estado cuja legislação restrinja a coleta de informações de nacionais pode receber esse tipo de informação de parceiros da rede, o que vale para todos seus integrantes.³¹⁸ Não bastasse, há evidências de que alguns governos têm sistematicamente conduzido operações de coleta e análise através de jurisdições com fracas garantias sobre o direito à privacidade.³¹⁹

Abordada a discussão sobre a licitude da coleta de informações privadas de particulares, na seção seguinte busca-se investigar possíveis abordagens conciliatórias entre o exercício da vigilância estatal em escala massiva com uma concomitante e adequada proteção ao direito à privacidade.

³¹⁷ [...] *digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant*". UNITED NATIONS GENERAL ASSEMBLY. **The right to privacy in the digital age**: Report... *op. cit.* p. 11-12, § 34.

³¹⁸ UNITED NATIONS GENERAL ASSEMBLY. **Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism**. *op. cit.* p. 16, § 44.

³¹⁹ UNITED NATIONS GENERAL ASSEMBLY. **The right to privacy in the digital age**: Report... *op. cit.* p. 10, § 30.

4.3.2 *Atritos entre privacidade e segurança: uma análise dos argumentos favoráveis à vigilância em massa*

A privacidade é uma faceta central de uma democracia liberal. Sistemas liberais de organização social reconhecem que os indivíduos que compõem a sociedade são independentes, autônomos uns em relação aos outros e em relação ao Estado. Essa autonomia significa liberdade de pensamento, escolha e ação; em essência, liberdade de ser. É o que garante um espaço de realização pessoal isento de interferência, o que só se concretiza se o indivíduo puder resguardar do conhecimento do público em geral aspectos de sua vida privada.³²⁰ De outra forma, como se garantir, por exemplo, o livre exercício de escolha política na ausência do sigilo dos votos, uma clara manifestação da privacidade individual? Como se proteger a liberdade de pensamento e crença se não se pode se abster de manifestá-los publicamente, resguardando-os ao foro privado?

Ocorre que, no atual paradigma tecnológico, que poderíamos caracterizar como a “era da informação”, é cada vez mais difícil perceber as reais nuances da relação entre a privacidade e as novas formas de comunicação digital. Grande parte das relações interpessoais acontecem hoje no ambiente cibernético de modo que uma quantidade imensa de informações é compartilhada digitalmente, permitindo seu fácil registro e monitoração pelo Estado ou empresas de comunicação. Nesse contexto, complexidades técnicas, de natureza tanto tecnológica quanto jurídica, fazem com que o público em geral tenha dificuldades em compreender com exatidão a legislação pertinente e a política de privacidade dos diversos serviços de comunicação via telefonia celular ou *internet*. Isso significa saber quais informações pessoais são armazenadas, quais podem ser divulgadas e sob quais circunstâncias. Da mesma forma, conceitos como os de criptografia, informações de *login*, geolocalização, apenas para exemplificar, são simplesmente ignorados pela maioria dos usuários desses serviços, muito embora interfiram diretamente na forma como as informações são compartilhadas. Esse panorama já levou muitos críticos a concluir que “a privacidade está morta”.³²¹

³²⁰ Para uma crítica ao modelo liberal de concepção da privacidade ler: COHEN, Julie E. What Privacy is For. **Harvard Law Review**, v. 26, 2013.

³²¹ Entre muitos outros exemplos: GARFINKEL, Simson. **Database Nation**: the death of privacy in the 21st Century. Sebastopol: O'Reilly, 2000; ROSEN, Jeffrey. **The Unwanted Gaze**: The Destruction of Privacy in America. New York: Vintage, 2001.

4.3.2.1 A falácia do argumento “Quem não deve não teme”

E assim a maioria das pessoas normalmente não se incomoda com violações à sua privacidade que não resultem em algum constrangimento ou prejuízo imediato. “Eu não tenho nada a esconder” e “Quem não deve não teme” são duas respostas frequentes a inquirições acerca da relevância da privacidade individual e autoridades estatais tendem a endossar essa espécie de justificativa. Na Inglaterra, após um atentado terrorista patrocinado pelo *Irish Republican Army (IRA)* em 1994 em que duas bombas explodiram no distrito financeiro de Londres, foi implementado um extenso programa de instalação de câmeras de vigilância nos principais pontos de acesso à cidade.³²² O *slogan* da bem sucedida campanha: “Se você não tem nada a esconder, não tem nada a temer”.³²³ Na academia também se manifestam opiniões coerentes com esse tipo de abordagem acerca da privacidade, do que é um bom exemplo a assertiva de Richard Posner para quem privacidade nada mais é que “um direito de esconder fatos desabonadores sobre si mesmo”.³²⁴

O problema central com esse tipo de argumentação é a premissa equivocada de que somente há interesse individual em ocultar fatos ilícitos ou imorais sobre si. A verdade é que todos temos algo a esconder, a começar pelos aspectos íntimos da imagem pessoal e da vida sexual. Com efeito – apesar de não se ter coletado dados para corroborar a afirmação seguinte – parece ser o caso de que a maioria das pessoas, ao descobrir uma foto de nudez ou mesmo um vídeo em que a mostra mantendo relações sexuais publicada em redes sociais sem sua autorização, irá buscar identificar o autor da publicação e ajuizar uma demanda pedindo sua condenação por danos morais bem como a retirada do material da *internet*. Uma hipótese mais extrema nos faz pensar que ninguém admitiria que o governo, tal como no clássico de George Orwell “1984”, instalasse em seu quarto uma câmera de vigilância ou mesmo tivesse acesso à câmera de seu *laptop* ou de seu *smartphone*.

³²² Dados de 2013 estimavam que havia 5.9 milhões de câmeras de circuito fechado no Reino Unido, o que representava 1 câmera para cada 11 cidadãos britânicos. BARRET, David. One surveillance camera for every 11 people in Britain, says CCTV survey. **The Telegraph**, 10 jul. 2013. Disponível em: <<http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html>>

³²³ “If you’ve got nothing to hide, you’ve got nothing to fear” ROSEN, Jeffrey. **The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age**. Random House Incorporated, 2005. p. 36.

³²⁴ “right to conceal discreditable facts about himself”. POSNER, Richard. **Economic Analysis of Law**. New York: Aspen, 5 ed, 1998. p. 46.

Se estas hipóteses da privacidade da imagem íntima parecem extremas e não suficientes para desafiar o argumento “quem não deve não teme”, basta recordar que informações pessoais sobre saúde, finanças e perfil de consumo, são alguns exemplos do que se busca ocultar do público em geral por razões de segurança e, em algumas situações, por respeito à dignidade. Ocorre que há um desafio na proteção dessas informações em virtude de seu valor comercial. Setores de mercado que lidam com o comércio de informações pessoais, os chamados *data brokers*, compilam listas de contatos de pessoas de acordo com determinada classificação, que são comercializadas a alguns centavos por nome. Algumas dessas listas mais preocupantes incluem endereços residenciais de oficiais de polícia, vítimas de estupro, locais de abrigos de vítimas de violência doméstica, portadores de doenças genéticas, idosos que sofrem de demência, portadores do vírus HIV e relações de pacientes com a respectiva medicação prescrita, tudo comercializado indiscriminadamente na rede.³²⁵

³²⁵ WORLD PRIVACY FORUM. **What Information Do Data Brokers Have on Consumers, and How Do They Use It?** Testimony of Pam Dixon Executive Director, World Privacy Forum, before the Senate Committee on Commerce, Science, and Transportation, 18 dez. 2013. Disponível em: <http://www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf>

AILMENTS MAILING LISTS / EMAIL LISTS

AILMENT / MEDICATIONS DATA SOURCE: Surveys and/or Data Contributions

IMPORTANT: When using the below ailments to create your new patient mailing list – be sure to use demographics to qualify your patients. Two patients with same medical ailment are not the same since they may have different demographics (age, income, education level, etc) ... and these demographics can influence the willingness to use your product/service.



CLICK HERE and receive a free count and quote for any ailment mailing list or email list .



CLICK HERE to review demographics for qualifying your ailment list.

TOP SELLING AILMENT EMAIL LISTS / MAILING LISTS

Wheelchair Users Mailing List: over 40,000
 Insulin Users Mailing List: over 400,000
 Back Pain Ailment Mailing List: over 3,000,000
 Sleep Apnea Mailing List: over 15,000
 Asthma Sufferers Mailing List: over 2,500,000
 Asthma Medication Users Mailing List: over 150,000
 Rheumatoid Arthritis Sufferers Mailing List: over 700,000
 Diabetics Mailing List: over 12,000,000
 Bladder Control Sufferers Mailing List: over 340,000
 ADHD Ailment Mailing List: over 500,000
 Clinical Depression Sufferers Mailing List: over 1,800,000

FREE MARKET COUNT

MASTER CONSUMER
DATABASE

CONSUMER LIST
QUALIFIERS

NEW HOMEOWNERS

CONSUMER EMAIL ADDRESSES

CONSUMERS BY LIFESTYLE

TOP EXECUTIVES
AT HOME ADDRESS

REAL ESTATE LEADS

(Captura de tela de uma página do *website dmdatabases.com*. Destaque para a relação das listas de e-mail de pacientes mais vendidas, entre elas a de usuários de cadeiras de rodas, diabéticos, e pessoas que sofrem de depressão. Disponível em: <<http://dmdatabases.com/databases/consumer-mailing-lists/ailments-lists>>)

Note-se ainda que a insegurança quanto à confidencialidade de informações pessoais produz efeitos em outros aspectos mais sutis, não obstante não menos relevantes. Como destaca Neil Richard, muitas pessoas que temem que seu comportamento na rede possa estar sendo monitorado pelo governo limitam sua atividade intelectual (o que lê ou escreve na *internet*) ao convencional, ao padrão. Tal constatação conta com evidências empíricas: em pesquisa realizada com 500 escritores americanos, muitos deles afirmaram que o medo da vigilância estatal limitou o que leram, escreveram ou disseram na *internet* (*chilling effects*).³²⁶ O mesmo efeito foi percebido em outro estudo, em que o alerta súbito a um grupo de pessoas entrevistadas de que suas manifestações estariam sujeitas à vigilância estatal fez com que opiniões divergentes a políticas públicas em condução (no caso

³²⁶ PEN AMERICAN CENTER. **Chilling Effects:** NSA Surveillance Drives U.S. Writers to Self-Censor, 2013. Cf. RICHARD, Neil M. *Four Privacy Myths In: SARAT, Austin [Org.]. A World Without Privacy: What Law Can and Should Do?* Cambridge University Press, 2015. p. 63.

o bombardeamento de alvos do *ISIS* pelos Estados Unidos), previamente consultadas no estudo, não fossem em sua maioria expressadas.³²⁷

O temor da vigilância é ainda agravado por aquilo que Daniel Solove denomina de problema da *distorção*. Ainda que a coleta de informações pessoais permita apontar diversos traços da personalidade e comportamento de um indivíduo, nada assegura que a análise que as autoridades estatais farão sobre essas informações conduzirão a conclusões corretas.³²⁸ Escritores e acadêmicos podem se sentir temerosos de que um histórico de frequentes pesquisas na *internet* sobre, por exemplo, armas químicas e biológicas ou processo de fabricação de explosivos – que iriam servir apenas para enriquecer uma reportagem, uma história fictícia ou mesmo um artigo científico – possa ser interpretado como indicativo de propósitos terroristas.

4.3.2.2 Os problemas em se relacionar “privacidade” e “segurança” sob uma ideia de balanceamento

Não resta dúvidas, portanto, que a privacidade é, de fato, um valor importante em uma sociedade democrática. Entretanto, por outro lado, argumenta-se que a promoção da segurança seria, de igual forma mas em maior medida, extremamente relevante para a defesa das instituições democráticas, que é mesmo a principal tônica do argumento favorável às atividades de vigilância estatal em escala massiva. Com efeito, como visto no capítulo 2, uma percepção de que serviços de inteligência não eram dotados de capacidades suficientes para impedir a ocorrência de ataques terroristas foi uma das principais conclusões alcançadas após os eventos. E assim formou-se a percepção de que um aumento dos poderes de serviços de inteligência contribuiria para evitar a prática de novos ataques.

Nesse contexto, o discurso de promoção da segurança tem um forte apelo pois se apresenta como medida de defesa da vida dos cidadãos, especialmente em um contexto de ameaça terrorista. Sob esse ponto de vista, a privacidade individual, um direito de suposta menor importância, não resistiria a um confronto com a proteção do valor supremo da vida. Seria justificável, como se argumenta, reduzir

³²⁷ STOYCHEFF, Elizabeth. Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring. **Journalism & Mass Communication Quarterly**, 2016.

³²⁸ SOLOVE, Daniel J. **Nothing to Hide**: The False Tradeoff between Privacy and Security, Yale University Press, 2011. p. 28.

um pouco da privacidade individual em prol da segurança coletiva. Nos termos colocados em tom crítico por Adam Moore: “Em tempos de crise nacional, cidadãos são frequentemente solicitados a trocar liberdade e privacidade por segurança. E por que não, argumenta-se, se nós podemos obter uma quantidade razoável de segurança por apenas um pouco de privacidade?”³²⁹

Autoridades estatais tendem a enxergar o problema sob a mesma ótica. O ex-Procurador-Geral dos Estados Unidos sob a gestão George W. Bush, Alberto Gonzales, certa vez afirmou em audiência no Congresso norte-americano: “Vocês querem que a gente pare de monitorar? Então os terroristas poderiam falar sobre como eles planejam explodir um avião, e nós não saberíamos sobre isso. Um pouco de privacidade realmente compensa esse custo?”.³³⁰

E assim, formula-se a relação entre privacidade e segurança em termos de balanceamento, o que exige aceitar a premissa de que o aumento da segurança deve, necessariamente, implicar diminuição da privacidade, ou vice-versa. Seriam, pois, valores antagônicos.

Todavia, há dois problemas graves no exercício de balanceamento entre privacidade e segurança que consistem em situar a análise do problema sob um critério de *hierarquização* e de *oposição*. Em primeiro lugar, mostra-se falho o argumento de que a segurança, ao proteger a vida, é um valor mais importante que a privacidade, pois esta também pode servir à proteção da vida. Na literatura norte-americana é célebre o caso do assassinato da atriz Rebecca Schaefer em julho de 1989, cujo autor descobriu o paradeiro da vítima através de informações pessoais obtidas junto ao departamento de trânsito. O trágico evento justificou a aprovação do *Drivers' Privacy Protection Act* de 1993.³³¹

É óbvio que o recurso a esse exemplo não é o mais adequado pois se trata de um evento isolado praticado por um particular, não uma forma de utilização indevida da informação por parte do Estado – muito embora a falta de segurança sobre a informação deva ser, no caso, atribuída ao Estado. Não obstante, o fato de eventuais erosões ao direito à privacidade serem conduzidas pelo Estado não

³²⁹ “In times of national crisis, citizens are often asked to trade liberty and privacy for security. And why not, it is argued, if we can obtain a fair amount of security for just a little privacy?”. MOORE, Adam D. Toward Informational Privacy Rights. **San Diego Law Review**, v. 44, 2007. p. 830.

³³⁰ “Do you want us to stop listening? Then the terrorists could talk about how they plan to blow up a plane, and we won’t know about it. Is a little privacy really worth that cost?” Cf. SOLOVE, D. *op. cit.* p. 34.

³³¹ NISSEMBAUM, Helen. Protecting Privacy in an Information Age: The Problem of Privacy in Public. **Law and Philosophy**, v. 17, 1998. p. 585.

garante, da mesma forma, que o sistema está isento de abusos. Em verdade, é a amplitude do poder estatal perante a população que preocupa em essência. Como reconhece Jeremy Waldron, a redução de liberdades civis pode aumentar a segurança e prevenir a ocorrência de ações potencialmente causadoras de dano, mas, segundo o autor, isso necessariamente implica aumento do poder do Estado e há um risco correspondente de que esse acréscimo de poder também seja utilizado para causar dano. Prossegue o autor:

A proteção de direitos civis não é apenas uma questão de nutrir certas liberdades que nós particularmente valorizamos. É também uma questão de desconfiança do poder, uma compreensão de que o poder dado ao Estado é raramente usado unicamente para os propósitos para os quais ele foi concedido, mas é sempre e endemicamente sujeito a abusos.³³²

Realmente, a história está repleta de exemplos de Estados que convertem o sistema de inteligência estatal em mecanismo de repressão e controle social, o que sempre vem precedido de graves violações à privacidade individual. O regime nazista com a *Gestapo*, a Alemanha oriental com a *Stasi*, a União Soviética com a *KGB*, o regime do *apartheid* na África do Sul e ditaduras militares como a brasileira e a chilena de Augusto Pinochet, são bons exemplos dos chamados “Estados Policiais”. Sabendo-se que em regimes autoritários as liberdades civis são quase sempre ignoradas e que não há garantias de que um governo democrático nunca irá se converter em uma ditadura ou mesmo nunca irá adotar políticas constritivas de liberdade, seria prudente velar pela privacidade enquanto as garantias vigentes de um Estado de Direito o permitem.

Um segundo problema com o raciocínio de se posicionar a relação entre privacidade e segurança em termos de balanceamento é a pressuposição de que o acréscimo de uma deve implicar necessariamente no decréscimo da outra e vice-versa. Sacrificar privacidade não nos torna automaticamente mais seguros; a divulgação dos dados bancários de uma pessoa, por exemplo, poderia representar risco à sua segurança pessoal. Da mesma forma, medidas de segurança não precisam necessariamente ser invasivas em relação à privacidade; atividades de

³³² “The protection of civil liberties is not just a matter of cherishing certain freedoms that we particularly value. It is also a matter of suspicion of power, an apprehension that power given to the state is seldom ever used only for the purposes for which it is given, but is always and endemically liable to abuse”. WALDRON, Jeremy. Security and Liberty: The Image of Balance. **The Journal of Political Philosophy**, v. 11, n. 2, 2003. p. 205.

patrulha policial de rotina em áreas públicas acresce à segurança de uma região sem afetar a privacidade das pessoas em sua residência.

Na verdade, privacidade e segurança podem se relacionar de forma complementar. Há situações em que maior segurança só pode ser obtida através de maior privacidade, do que seria um bom exemplo o uso da criptografia na proteção de sistemas informáticos do governo contra invasores estrangeiros. Provavelmente representa ela também o melhor ponto de discussão sobre a relação entre privacidade e segurança. Isso porque, é preciso que se reconheça, que a mesma criptografia que protege sistemas governamentais, é aquela que resguarda comunicações privadas de um cidadão inocente ou os dados de um terrorista ou redes de Estados e grupos hostis. É possível notar então que a criptografia, como um conceito, é valorativamente neutra, ou seja, não é o caso de se definir se ela é boa ou má, mas sim de compreender que ela pode ser favorável ao não à realização de determinados propósitos específicos e, nesse sentido, regular sua utilização.

De fato, agências de inteligência, com uma boa carga de razão, se manifestam enfaticamente contrárias à utilização de uma criptografia forte em aparelhos celulares e computadores pessoais, o que na sua visão dificulta o combate ao terrorismo. Como declarou o Diretor da NSA, almirante Michael Rogers em entrevista, quando perguntado sobre o impacto que a criptografia produz nas atividades da agência:

É mais difícil para nós gerar o tipo de conhecimento que eu gostaria sobre alguns desses alvos? Sim. Isso está diretamente ligado em parte às mudanças que eles estão fazendo em suas comunicações? Sim. A criptografia torna muito mais difícil para nós executar nossa missão? Sim.³³³

O almirante afirmou inclusive que algumas das comunicações dos terroristas responsáveis pelos ataques de novembro de 2015 em Paris (seção 2.2) estavam criptografadas e, como consequência, não foi possível antecipar a ação. Segundo

³³³ *"Is it harder for us to generate the kind of knowledge that I would like against some of these targets? Yes. Is that directly tied in part to changes they are making in their communications? Yes. Does encryption make it much more difficult for us to execute our mission? Yes."* (Michael Rogers) ISIKOFF, Michael. NSA chief: 'Paris would not have happened' without encrypted apps. **Yahoo! Politics**, 17 fev. 2016. Disponível em: <<https://www.yahoo.com/politics/nsa-chief-paris-would-not-have-happened-without-184040933.html>>

ele, “claramente, se nós soubéssemos, Paris não teria acontecido”.³³⁴ O Diretor ainda relacionou as revelações de Snowden com uma postura de organizações terroristas mais preocupada em proteger suas comunicações.

Viu-se a al-Qaida expressamente, por exemplo, mencionar as divulgações [de Snowden]. Viu-se grupos – ISIS fez o mesmo – falarem sobre como eles precisam mudar sua disciplina, precisam mudar sua segurança como resultado de um maior conhecimento sobre o que nós fazemos e como fazemos. [...] Ninguém deve duvidar por um minuto sequer que houve um impacto nisso. Eu deixarei para outros decidirem se foi certo, errado, bom ou mal. Mas não deve haver qualquer dúvida na mente de qualquer pessoa de que houve um impacto como resultado dessas divulgações.³³⁵

O fato é que a criptografia de aparelhos de comunicação existe para proteger finalidades legítimas de segurança de dados e privacidade, como por exemplo sigilo de dados em operações bancárias ou pagamentos no comércio eletrônico feitos em celulares ou computadores. Ela evita, principalmente, que *hackers* invadam o sistema de tais aparelhos para propósitos criminosos, mas nada impede, por outro lado, que terroristas se utilizem da mesma proteção para o planejamento e execução de ataques. É óbvio que não se quer uma criptografia fraca o bastante a permitir que criminosos obstruam com facilidade um sistema, mas isso por vezes a torna forte o suficiente a impedir que o governo não possa investigar o celular de alguém com comprovados vínculos com organizações terroristas.

Esse atrito se concretizou recentemente na resistência da *Apple* em cumprir uma ordem judicial do distrito central da Califórnia, que determinava que a companhia deveria colaborar com autoridades do *FBI* para o desbloqueio de um celular *Iphone 5c* utilizado por um dos atiradores do massacre de San Bernardino, em dezembro de 2015. A resistência da *Apple* em desbloquear o aparelho, justificada pela política da empresa em nunca atuar no sentido de reduzir a segurança de seus produtos e sempre em defesa da privacidade de seus

³³⁴ “we did not generate the insights ahead of time. Clearly, had we known, Paris would not have happened.” *Ibidem*.

³³⁵ “You’ve seen al-Qaida expressly, for example, reference the disclosures. You’ve seen groups — ISIL does the same — talk about how they need to change their discipline, need to change their security as a result of their increased knowledge of what we do and how we do it. [...] “No one should doubt for one minute there has been an impact here. I will leave it to others to decide right, wrong, good or bad. But there shouldn’t be any doubt in anybody’s mind that there has been an impact as a result of these disclosures.” *Ibidem*.

consumidores – foi respondida pelo Departamento de Justiça dos Estados Unidos com uma ação na justiça federal, posteriormente retirada uma vez que o *FBI* conseguiu vencer a criptografia do celular.³³⁶ Note-se que a questão não se encerrou na definição da licitude da recusa da *Apple* em colaborar com as autoridades ou mesmo na própria licitude do desbloqueio do celular pelo *FBI*, mas sim na sua competência técnica em fazê-lo.

Um outro bom exemplo desse conflito é ilustrado pela utilização de *softwares* que aumentam as chances do usuário realizar uma navegação anônima pela *internet*, ao dificultar o rastreamento de sua localização e identidade pelos *websites* acessados.³³⁷ O recurso a esse tipo de *software* favorece a navegação à *deep web*, que é o nome que se atribui ao conjunto de *websites* que não podem ser encontrados através de um mecanismo de busca comum como o *google* ou o *bing*. Dado o anonimato de navegação, esse espaço favorece práticas criminosas como comercialização ilícita de drogas, armas e informações, sendo ainda uma ambiente fértil para a disseminação de ideologias extremistas.³³⁸

Um outro argumento favorável às atividades de vigilância em massa passa por uma explicação mais clara do que efetivamente consistem esses programas dentro da estrutura de uma agência de inteligência. Essa explicação compreende o fato de que a escala massiva da vigilância se refere à sua abrangência, horizontalidade, não à sua profundidade, verticalidade. Os dados coletados em escala massiva se referem ao processo da comunicação, os chamados metadados, e não ao conteúdo da comunicação em si, esse apenas analisado de forma direcionada a indivíduos específicos, sob autorização judicial domesticamente, ou sem necessidade de autorização em relação a pessoas que se encontram fora dos Estados Unidos. (cf. seção 3.1) Como explicou o ex-Diretor de Inteligência Nacional James Clapper:

³³⁶ LESWING, Kif. The FBI says it has hacked into the San Bernardino shooter's phone without Apple's help. **Business Insider**, 28. Mar. 2016. Disponível em: <<http://www.businessinsider.com/the-government-is-reportedly-ending-its-quest-to-have-apple-help-it-access-data-on-an-encrypted-iphone-2016-3>>

³³⁷ Por exemplo, o *software* TOR (*The Onion Router*). Cf. TOR PROJECT. Disponível em: <www.torproject.org>

³³⁸ Um relatório preparado pelo *Institute for Security Studies*, da União Europeia, datado de 2015, evidenciava uma crescente penetração de organizações terroristas em *websites* da *Deep Web*. Cf. BERTON, Beatrice. The dark side of the web: ISIL's one-stop shop? **EUISS Alert**, Institute for Security Studies, European Union, v. 30, 2015. Disponível em: <http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf>

Apesar desse programa ter sido propriamente classificado, o vazamento de uma ordem [judicial], fora de qualquer contexto, criou uma impressão equivocada de como ele opera. Dessa forma, nós determinamos a desclassificação de algumas informações limitadas sobre esse programa. O programa não permite que o Governo escute as ligações de telefone de qualquer pessoa. A informação adquirida não inclui o conteúdo de quaisquer comunicações ou a identidade de qualquer assinante. O único tipo de informação adquirida sob a ordem da Corte são metadados de telefonia, tais como os números discados e a duração das chamadas. A coleta é ampla em alcance porque uma coleta mais estreita limitaria nossa habilidade de rastrear e identificar comunicações relacionadas ao terrorismo. Adquirir essa informação nos permite fazer conexões relacionadas a atividades terroristas ao longo do tempo.³³⁹

Isso sustenta o argumento segundo o qual, sendo a vigilância em escala massiva dirigida apenas à coleta de metadados e não ao conteúdo de comunicações, não haveria qualquer prejuízo à privacidade individual. De fato, os metadados, analisados isoladamente, não dizem muita coisa a respeito dos interlocutores de uma comunicação. Todavia, quando relacionados, podem revelar informações sobre uma pessoa a níveis de afetar significativamente sua privacidade. Confira-se o que exatamente compreendem os metadados³⁴⁰:

- A localização dos dispositivos envolvidos na comunicação;
- A localização precisa do dispositivo quando é feita a checagem de novos e-mails ou publicações em redes sociais;
- Números de identificação dos dispositivos, e.g. o *IMEI – International Mobile Station Equipment Identity*;
- O horário das ligações ou mensagens enviadas e recebidas;
- Duração das ligações

³³⁹ “Although this program has been properly classified, the leak of one order, without any context, has created a misleading impression of how it operates. Accordingly, we have determined to declassify certain limited information about this program. The program does not allow the Government to listen in on anyone’s phone calls. The information acquired does not include the content of any communications or the identity of any subscriber. The only type of information acquired under the Court’s order is telephony metadata, such as telephone numbers dialed and length of calls. The collection is broad in scope because more narrow collection would limit our ability to screen for and identify terrorism-related communications. Acquiring this information allows us to make connections related to terrorist activities over time”. CLAPPER, James. **DNI Statement on Recent Unauthorized Disclosures of Classified Information**, Office of the Director of National Intelligence, 06 jun. 2013. Disponível em: <<http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information>>

³⁴⁰ Adaptado de PRIVACY INTERNATIONAL. **Metadata**. Disponível em: <<https://www.privacyinternational.org/node/53>>

- Quantidade de dados transmitidos em cada comunicação
- Informações relacionadas aos interlocutores, como endereço de *e-mail*, endereço de IP, servidores, lista de contatos;

A correlação desses dados pode conduzir a conclusões surpreendentes. Ao associar a identidade de uma pessoa com os locais que ela frequenta e com os respectivos horários é possível traçar um perfil de seu hábitos e preferências, ou identificar outras pessoas com quem ela se reúne. Segundo o Diretor do Centro para Políticas de Tecnologia da Informação da Universidade de Princeton, Edward Felten, ligações destinadas a programas de doações pode revelar preferências políticas e a data de ligações pode evidenciar crenças religiosas (muitas ligações no natal ou nenhuma ligação durante o *Sabbath*).³⁴¹ A matemática e engenheira Susan Landau apresenta a hipótese em que um padrão de frequentes ligações entre dois executivos de grandes empresas indica possíveis negociações de fusões e aquisições. Em outro exemplo, sugere uma ligação feita para um oncologista seguida de outra feita a familiares próximos, a indicar um possível diagnóstico de câncer. Metadados também representam risco, lembra a autora, à atividade jornalística, pois podem revelar a localização e identidade de fontes.³⁴²

Além dos riscos à privacidade que o programa de coleta massiva de metadados representa, não há demonstração empírica de que esse método produz acréscimo significativo à segurança, com exemplos concretos em que contribuiu para o combate ao terrorismo. O próprio Relator Especial da ONU para Privacidade, Joseph Cannataci, afirmou que ainda não encontrou evidência de que a vigilância em massa seja necessária.³⁴³

É preciso reconhecer que, na esfera da persecução penal, há evidências de que a vigilância em massa produz resultados favoráveis. Susan Landau afirma

³⁴¹ LITHWICK, Dahlia; VLADECK, Steve. Taking the “Meh” out of Metadata. **Slate**, 22 nov. 2013. Disponível em: http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html>

³⁴² MAYER, Jane. What’s the Matter with Metadata? **The New Yorker**, 6 jun. 2013. Disponível em: <http://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata>>

³⁴³ “It can be necessary and proportionate to have targeted surveillance and what I am saying is that there’s not yet any evidence which convinces me that it is necessary and proportionate to have mass surveillance.” (Joseph Cannataci). BURGESS, Matt. UN privacy chief: UK surveillance bill is ‘worse than scary’. **Wired**, 10 nov. 2015. Disponível em: <http://www.wired.co.uk/news/archive/2015-11/10/surveillance-investigatory-powers-scary-joseph-cannataci>>

que a coleta de metadados de localização de celulares reduziu o tempo médio de captura de fugitivos pelos *U.S. Marshals* de 42 dias para apenas 2.³⁴⁴ Mas um ganho geral em segurança com a coleta massiva de metadados, que seria principalmente representado pela obstrução tempestiva de ataques terroristas, ainda não foi devidamente comprovado.

Por outro lado, deve-se notar o fato de que as operações de inteligência são sigilosas e talvez por isso não se possa identificar o ganho que operações de vigilância em massa representam concretamente para a segurança nacional. Para que uma agência demonstre efetivamente como um ataque terrorista foi impedido graças a informações obtidas através da coleta massiva de metadados teria ela que divulgar detalhes classificados sobre suas operações, o que colocaria em risco o êxito de operações futuras. Com efeito, é possível que haja ações bem sucedidas de obstrução de ataques terroristas das quais o público em geral não toma conhecimento. Isso faz com que o argumento segundo o qual não há comprovação empírica de que a vigilância em massa produz um ganho significativo para a segurança deva ser considerado com cautela.

Vale observar, no entanto, que um estudo da *New America Foundation* conduzido sobre 225 casos envolvendo pessoas ligadas ao terrorismo (indiciadas, condenadas ou mortas pelas autoridades) nos Estados Unidos entre setembro de 2001 e o final de 2013, concluiu que em apenas 7.5% deles informações fornecidas pela NSA permitiram o início de uma investigação, sendo que a coleta massiva de metadados de telefonia contribuiu com somente 1.8% do total. A maioria dos casos foram deflagrados por métodos tradicionais de investigação.

Métodos que deflagraram investigações de terrorismo nos Estados Unidos (2001- 2013)³⁴⁵

³⁴⁴ LANDAU, Susan. **Surveillance or Security**. Massachusetts Institute of Technology Press, 2010. p. 261.

³⁴⁵ Adaptado de BERGEN, Peter; STERMAN, David; SCHNEIDER, Emily; CAHALL, Bailey. Do NSA's Bulk Surveillance Programs Stop Terrorists? **New America Foundation**, jan. 2014. Disponível em: <https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf> Sobre os casos em que houve dúvidas sobre o método de início da investigação, esclareceram os pesquisadores: “The unclear cases may have been initiated by an undercover informant, a family member tip, other traditional law enforcement methods, CIA or FBI generated intelligence, NSA surveillance of some kind, or any number of other methods. Additionally, some of these cases may be too recent to have developed a public record large enough to identify which investigative tools were used. In 23 of these 62 unclear cases (37 percent), an informant was involved, though we were unable to determine whether the informant initiated the investigation. The widespread use of informants suggests that if there was an NSA role

Método	Nº de Casos	% do Total
Informação da família / comunidade	40	17.8%
Coleta massiva de metadados pela NSA (seção 215, PATRIOT ACT)	4	1.8%
Vigilância de cidadãos estrangeiros pela NSA (seção 702, FISA)	10	4.4%
Vigilância pela NSA sob autoridade legal desconhecida	3	1.3%
Informantes	36	16%
Informação de outras agências de inteligências (CIA, FBI etc.)	18	8%
Persecução penal de rotina	12	5.3%
Informação voluntariamente divulgada pelo terrorista	9	4%
Relato de atividade suspeita	19	8.4%
Dúvidas sobre o método	62	27.6%
Ação terrorista não obstruída	12	5.3%
	Total	
	225	

Por razões semelhantes, o Grupo de Revisão de Serviços de Inteligência e Comunicação, convocado pelo ex-presidente Barack Obama após as revelações de Snowden, também reconheceu que não há justificativas para a manutenção do programa de coleta massiva de metadados de telefonia, sugerindo sua revogação.³⁴⁶ Com efeito, a estratégia de monitoração de dados de comunicações justificaria sua utilidade para a identificação de suspeitos que possuem algum vínculo e mantêm contato com uma organização ou célula terrorista. Mas o crescimento nos últimos anos do número de ataques de autoria dos chamados “lobos solitários” – que são aqueles indivíduos que, seduzidos por ideologias extremistas com que têm contato pela *internet* e sem nunca terem feito qualquer comunicação com grupos radicais, se lançam à prática independente de um ato terrorista – sugere que a monitoração do comportamento dos indivíduos na rede passará a ser um método a que as agências de inteligência recorrerão com maior frequência.

Por tudo que se disse, pode-se concluir que é preciso analisar com cautela medidas de limitação à privacidade quando justificadas em uma suposta superioridade do valor “segurança”. Tanto “privacidade” quanto “segurança” podem servir, inclusive de forma complementar, à proteção de valores mais centrais como “vida” e “liberdade”. Qualquer argumento que pretenda converter a relação entre

in these cases, it was limited and insufficient to generate evidence of criminal wrongdoing without the use of traditional investigative tools”.

³⁴⁶ “In light of these alternatives, we conclude that there is no sufficient justification for allowing the government itself to collect and store bulk telephony meta-data. We recommend that this program should be terminated as soon as reasonably practicable”. CLARKE R. A. et. al. op. cit. p. 119.

esses dois valores em um “jogo de soma zero”, uma “balança de troca” na qual o aumento de um significa a redução de outro, provavelmente não revelará as verdadeiras nuances da questão. Não se quer dizer com isso que qualquer raciocínio de balanceamento entre privacidade e segurança será equivocado, mas apenas que há situações em que essa forma de pensar o problema não é adequada e em outras sim.

De qualquer forma, um modo seguro de pensar o problema se dá através da aceitação de que pretensões legítimas de limitação à privacidade – o mesmo raciocínio vale para qualquer outra liberdade civil – em favor da segurança somente podem ser construídas sobre uma criteriosa demonstração de que a) há real necessidade por acréscimo na segurança; b) esta não pode ser suprida sem intervenção na privacidade e c) a intervenção no exercício da privacidade efetivamente implicará um ganho em segurança. Como alerta Jeremy Waldron, essas ponderações precisam ser feitas de forma honesta. É preciso se estar seguro de que diminuição de liberdades tenham a consequência esperada. E, caso o almejado resultado não possa ser antecipado com certeza, mas apenas em níveis de probabilidade, então é preciso ser o mais transparente possível sobre a extensão dessa probabilidade.³⁴⁷

4.4 A discussão sobre a licitude da espionagem econômica³⁴⁸

Das modalidades de espionagem, aquela em que mais facilmente se percebe a ilegitimidade é a espionagem econômica. Isso porque seu objetivo é a coleta de informações que tem um valor intrínseco, não relacionado à orientação do processo decisório de autoridades estatais, nem mesmo a finalidades ligadas à promoção da segurança nacional. Como ficou claramente demonstrado na seção 3.2, a razão de ser da espionagem econômica é a obtenção clandestina de uma vantagem concorrencial – um método desleal.³⁴⁹

³⁴⁷ WALDRON, J. *op. cit.* p. 208-209.

³⁴⁸ Boa parte do que aqui se discute foi objeto de publicações anteriores de nossa autoria em: LIMA, H. A. V.; CUNHA, N. M. R. *op. cit.*

³⁴⁹ Há quem argumente que a espionagem econômica é, além de um meio de obtenção de vantagem competitiva, uma extensão da rivalidade militar, que serve o propósito de evitar o conflito bélico enquanto for possível manter a dominação sobre o Estado competidor. CROSTON, Matthew. *Soft Spying: Leveraging Globalization as Proxy Military Rivalry*. **International Journal of Intelligence and CounterIntelligence**, v. 28, n. 1, 2015.

Apesar de atividades de concorrência desleal poderem ser exercidas de muitas maneiras e sobre informações diversas, aqui se restringe a análise da espionagem econômica quando dirigida a segredos de empresa, uma espécie protegida pelos direitos de propriedade intelectual. Portanto, a questão que se apresenta é a de saber se há normas de direito internacional que seriam aplicáveis às atividades de obtenção clandestina de segredo de empresa conduzidas ou patrocinadas por um Estado contra uma empresa³⁵⁰, seja ela pública ou privada e, caso haja, especificar quais são elas.

4.4.1 *A natureza concorrencial do segredo de empresa e sua categorização como espécie de propriedade intelectual*

De forma genérica, segredo de empresa é aquela informação que possuirá valor concorrencial enquanto sigilosa for. Ou, nas palavras de Deborah Bouchoux, “o tipo de informação que precisa ser mantida confidencial para reter sua vantagem competitiva”.³⁵¹ Com efeito, o detentor desse tipo de informação tem um interesse legítimo e juridicamente protegido em mantê-la sob segredo, pois, caso seu concorrente dela tome conhecimento, a vantagem concorrencial alcançada graças a dispendiosos investimentos ou um avanço inovador desaparecerá, causando um desequilíbrio favorável ao competidor – o chamado *free riding*.

Naturalmente, do ponto de vista concorrencial, há um risco inerente ao processo de manutenção de informações sob segredo. Pense-se, por exemplo, em uma empresa que desenvolve um novo combustível automotivo. Ela tem a opção, de um lado, de solicitar uma patente do produto – caso em que a tecnologia será publicada – e assim se beneficiar de um período limitado de exclusividade em sua exploração econômica ou mesmo licenciar, neste mesmo prazo, a tecnologia para concorrentes, como fonte de *royalties*. De outro lado, pode optar por manter a fórmula do combustível sob segredo de empresa indefinidamente e com isso auferir uma vantagem competitiva sobre outras empresas do mesmo setor enquanto for capaz de sustentar a confidencialidade. Ocorre que, neste último caso, se a

³⁵⁰ Recorde-se que, como frisado na seção III da Metodologia, acerca dos limites materiais da tese, a pesquisa engloba atos de espionagem conduzidos pelos Estados (sujeito ativo) que tenham por alvo tanto outro Estado quanto o particular, seja ele pessoa natural ou jurídica. (sujeitos passivos).

³⁵¹ “The type of information that must be kept confidential in order to retain its competitive advantage”. BOUCHOUX, Deborah E. **Intellectual Property: The Law of Trademarks, Copyrights, Patents and Trade Secrets**. 4 ed., Delmar Cengage Learning, 2013. p 469.

tecnologia for desenvolvida por concorrentes de forma independente, sem recurso a artifícios de concorrência desleal, a vantagem competitiva do titular do segredo se perde.

Cada Estado define os tipos de informação que irá tutelar como segredo de empresa – uma escolha de política econômica – e as consequências de sua obtenção ilícita de modo que a licitude doméstica do ato irá variar de país para país.³⁵² O principal tratado internacional de proteção aos direitos de propriedade intelectual, o acordo TRIPS (*Trade-Related Aspects of Intellectual Property Rights*), um dos anexos do GATT (*General Agreement on Tariffs and Trade*), estabelece um patamar mínimo de tutela a tecnologias e outras formas de produção intelectual – invenções, direitos de autor, marcas, indicações geográficas, desenho industrial, topografias de circuitos integrados, informações confidenciais e concorrência desleal – que os Estados signatários devem realizar internamente, através de sua legislação doméstica. Não obstante, os Estados podem estabelecer níveis de proteção maiores que os parâmetros mínimos definidos no TRIPS, mas nunca inferiores.³⁵³ Os Estados Unidos, por exemplo, adotam uma categorização ampla de segredos de empresa, definidos no *Economic Espionage Act* de 1996 como sendo:

“[...] todas as formas e tipos de informação financeira, comercial, técnica, econômica ou de engenharia, incluindo-se padrões, planos, compilações, dispositivos de programa, fórmulas, desenhos, protótipos, métodos, técnicas, processos, procedimentos, programas ou códigos, tangíveis ou intangíveis, tanto estocado, quanto compilado ou memorizado, fisicamente, eletronicamente, graficamente, em fotografia, ou em escrita [...]”.³⁵⁴

Em nível internacional, a seção 7 do acordo TRIPS, sob a epígrafe “Proteção de Informação Confidencial”, não define um conceito de segredos de empresa ou

³⁵² No Brasil, a Lei 9.279/96 (Lei Brasileira de Propriedade Industrial), tipifica como crime de concorrência desleal, em seu art. 195, incisos XI, XII, XIII e XIV, atos de divulgação, exploração ou utilização de segredos de empresa.

³⁵³ O art. 1(1) do Acordo define que: “1. Os Membros colocarão em vigor o disposto neste Acordo. Os Membros poderão, mas não estarão obrigados a prover, em sua legislação, proteção mais ampla que a exigida neste Acordo, desde que tal proteção não contrarie as disposições deste Acordo. Os Membros determinarão livremente a forma apropriada de implementar as disposições deste Acordo no âmbito de seus respectivos sistema e prática jurídicos”.

³⁵⁴ “the term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing [...]”. UNITED STATES OF AMERICA. **US Code**, Título 18, Parte I, Capítulo 90, § 1839, item 3.

um rol exemplificativo de seu conteúdo, tal como a legislação estadunidense, mas impõe aos seus signatários o dever protegê-los, atendidos três requisitos, como previsto no art. 39 (2):

2. Pessoas físicas e jurídicas terão a possibilidade de evitar que informação legalmente sob seu controle seja divulgada, adquirida ou usada por terceiros, sem seu consentimento, de maneira contrária a práticas comerciais honestas, desde que tal informação:
 - (a) seja secreta, no sentido de que não seja conhecida em geral nem facilmente acessível a pessoas de círculos que normalmente lidam com o tipo de informação em questão, seja como um todo, seja na configuração e montagem específicas de seus componentes;
 - (b) tenha valor comercial por ser secreta; e
 - (c) tenha sido objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta.³⁵⁵

Considerado o teor do dispositivo, o problema da licitude da espionagem econômica internacional exige definir a aptidão ou não da regra para tornar proscria a atividade de acordo com o Direito Internacional. Em termos mais simples, o artigo 39 (2) do acordo TRIPS proíbe atos de espionagem econômica entre os Estados? A resposta a essa pergunta passa pelo reconhecimento de que o regime de proteção internacional da propriedade intelectual está simbioticamente relacionado ao Direito do Comércio Internacional e, por essa razão, justifica-se um exame mais acurado dessa relação antes de formular qualquer conclusão a respeito do problema.

4.4.2 O vínculo entre Propriedade Intelectual e Comércio Internacional³⁵⁶

Há uma relação material entre propriedade intelectual e comércio internacional que se estabelece quando a ausência de proteção à propriedade intelectual em determinado país representa uma barreira ao comércio de produtos originados de um segundo país em que estes direitos são protegidos.³⁵⁷ Isso ocorre porque produtos protegidos por propriedade intelectual naturalmente refletirão um

³⁵⁵ ORGANIZAÇÃO MUNDIAL DO COMÉRCIO. **Acordo Sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio**, 1994. art. 39 (2).

³⁵⁶ Parte do que se diz nessa seção foi publicado anteriormente em LIMA, Humberto Alves de Vasconcelos. A construção do vínculo entre propriedade intelectual e comércio internacional e seus reflexos no Brasil. **Revista Eletrônica Direito e Política**, v. 9, n. 2, 2014. Disponível em: <<http://www6.univali.br/seer/index.php/rdp/article/view/6033>>

³⁵⁷ MATSUSHITA, Mitsuo; SCHOENBAUM, Thomas J.; MAVROIDIS, Petros C. **The World Trade Organization: Law, Practice and Police**. Oxford: Oxford University Press, 2006. p. 397.

preço mais elevado que produtos análogos que desempenham a mesma função mas não concentram os gastos com pesquisa e desenvolvimento, com criação de marca e com o patenteamento em relação ao que aqueles demandaram. Pense-se, por exemplo, em uma empresa britânica que desenvolva um medicamento inovador para o tratamento da hipertensão. O preço deste medicamento irá refletir todos os gastos expendidos com a pesquisa e o desenvolvimento do composto, com a criação e registro da marca e com o patenteamento do produto (custos estes que aumentam em proporção direta ao número de países em que se pretende ver protegido o produto por propriedade intelectual). Agora suponha-se que essa mesma empresa pretenda vender seu produto em um país em que medicamentos não se incluem no âmbito de patenteabilidade definido pela lei. Nesse Estado, a empresa britânica não conseguirá competir com outras empresas que poderão produzir e comercializar o mesmo composto a preços inferiores, uma vez que não precisarão amortizar os mesmos gastos que a primeira suportou.

Por perceberem essa relação, os países desenvolvidos – na posição de grandes exportadores de tecnologia e de produtos inovadores – buscaram inserir normas de proteção à propriedade intelectual no compromisso de liberação do comércio internacional, ao aprovarem o GATT de 1994 na Rodada de Negociações do Uruguai. Disto resultou a formalização do acordo TRIPS – vínculo formal inédito entre propriedade intelectual e comércio internacional – ajustado no desejo de seus signatários de reduzir distorções e obstáculos ao comércio internacional, promover uma proteção eficaz e adequada dos direitos de propriedade intelectual e assegurar que as medidas e procedimentos destinados a fazê-los respeitar não se tornem, por sua vez, obstáculos ao comércio legítimo.³⁵⁸

Obviamente, os segredos de empresa operam sobre uma lógica diferente das tecnologias patenteadas, pois seu valor reside justamente na sua confidencialidade e sua proteção é indefinida, limitada apenas pela capacidade de seu titular de sustentar seu sigilo e pelas regras de proteção à concorrência desleal. Não obstante, a função da proteção dos segredos de empresa no contexto do comércio internacional é a mesma que a de todas as espécies de propriedade intelectual: impedir que a concorrência, seja ela desleal – no caso de apropriação ilícita de segredos de empresa – ou mesmo “desequilibrada”, por assim dizer, no caso de

³⁵⁸ ORGANIZAÇÃO MUNDIAL DO COMÉRCIO. **Acordo...** *op. cit.* Preâmbulo.

Estados que não oferecem proteção patentária – se converta em barreira ao livre comércio.

Seguindo essa mesma lógica, ao verificar a investida da espionagem econômica chinesa contra as empresas dos Estados Unidos, como descrito na Introdução, vozes no congresso norte-americano³⁵⁹, na sociedade civil³⁶⁰ e na academia³⁶¹ sugeriram que uma reação adequada consistiria em apresentar a questão ao Órgão de Solução de Controvérsias da OMC. A opção não chegou a se realizar, mas vale aqui analisar a viabilidade dessa pretensão, ainda com o propósito de definir a licitude de atividades de espionagem econômica segundo o Direito Internacional.

4.4.3 *A proteção da informação confidencial no acordo TRIPS e as atividades de espionagem econômica no contexto do comércio internacional*

Como visto, o art. 39 (2) do acordo TRIPS oferece proteção às informações confidenciais de valor comercial. Isso significaria uma proibição de atos de espionagem econômica entre os Estados, autorizando a OMC a apreciar casos que a envolvam?

As normas e procedimentos sobre solução de controvérsias da OMC se aplicam a todos os acordos que compõem o GATT/1994 e ao acordo constitutivo da Organização (“Tratado de Marraquexe”), como definido em seu Anexo 2 (Entendimento Relativo às Normas e Procedimentos sobre Solução de Controvérsias), Artigo 1 e Apêndice 1. Abrangem, portanto, o acordo TRIPS, de sorte que o órgão de solução de controvérsias é competente para apreciar litígios envolvendo propriedade intelectual. Com efeito, como observa John Jackson, “virtualmente qualquer aspecto de regulação e política econômica é tocado, ao

³⁵⁹ Em 22 de maio de 2014, o Senador Charles E. Schumer enviou uma carta ao *U.S. Trade Representative*, Michael Froman, solicitando que a questão da espionagem econômica chinesa fosse apresentada à OMC. A carta pode ser lida em: <http://www.schumer.senate.gov/Newsroom/record.cfm?id=351779>

³⁶⁰ Cf. LEWIS, James A. **Conflict and Negotiation in Cyberspace**. Washington: Center for Strategic and International Studies, 2013. p. 49.

³⁶¹ SKINNER, Christina Parajon. An International Law Response to Economic Cyber Espionage. **Connecticut Law Review**, v. 46, n. 4, 2014.

menos potencialmente, se não de fato”.³⁶² Logo, em princípio a OMC seria competente para apreciar atividades de espionagem econômica, desde que, obviamente, se caracterize anteriormente uma violação a um dos acordos da OMC.

Dessa forma, resta saber se a espionagem econômica internacional consiste em uma violação ao art. 39 do acordo TRIPS. Um argumento contrário à verificação de uma violação nessa hipótese vem sendo defendido por David Fidler, de acordo com o seguinte raciocínio:

Uma razão pela qual membros da OMC não tem recorrido à Organização é a dificuldade de formular alegações de que a espionagem econômica viola os acordos da OMC. As regras da OMC criam obrigações aos seus membros a serem cumpridas em seus territórios e geralmente não impõem deveres que se aplicam fora desse limite. Os membros da OMC que obtém ocultamente propriedade intelectual de nacionais de outro membro operando em seus territórios poderiam violar obrigações de proteger tal propriedade. No entanto, a espionagem econômica de maior preocupação – e especialmente atos de espionagem cibernética conduzidos remotamente – envolve governos obtendo informação de companhias do setor privado localizadas fora de seu território.³⁶³

Vejamos as consequências práticas do argumento de David Fidler. Segundo o autor, as regras da OMC (dentre elas o acordo TRIPS), vinculam a seus membros

³⁶² “virtually every aspect of economic regulation and policy is touched upon at least potentially, if not actually [...]” JACKSON, John H. **Sovereignty, the WTO and Changing Fundamentals of International Law**. Cambridge: Cambridge University Press, 2006. p. 135.

³⁶³ “One reason why WTO members have not used the WTO is the difficulty of formulating claims that economic espionage violates WTO agreements. WTO rules create obligations for WTO members to fulfill within their territories and do not generally impose duties that apply outside those limits. WTO members that covertly obtain intellectual property of nationals of other WTO members operating in their territories could violate WTO obligations to protect such property. However, the economic espionage of greatest concern—and especially acts of remotely conducted economic cyber espionage—involves governments obtaining information from private-sector companies located outside their territories”. FIDLER, David. P. Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies. **American Society of International Law Insights**, v. 17, n. 10, 2013. Disponível em: <<http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving>> Em outro texto o autor reafirma a mesma conclusão: “Nothing in the WTO generally or TRIPS specifically mandates that China (or any other WTO member) protect commercially valuable information found in the territories of other countries. TRIPS does not require WTO members to prohibit their nationals or companies from engaging in corporate espionage inside foreign nations, nor does TRIPS regulate government-led economic espionage within other countries. Thus, the US cannot claim that China is violating TRIPS with respect to Chinese economic cyber espionage the US fears is most damaging to US economic and commercial interests. Or, put another way, China has not made commitments under the WTO regarding espionage it conducts outside its territory, meaning the US cannot claim breach of legal obligations that justifies countermeasures involving trade restrictions against China”. FIDLER, D. P. Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage. **Arms Control Law**, 11 fev. 2013. Disponível em: <<http://armscontrolaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>>

obrigações a serem adimplidas territorialmente. Dessa forma, acompanhando o raciocínio com a proposição de um exemplo, se o Estado chinês decidir patrocinar atividades de espionagem econômica contra a *General Electrics (GE)*, uma empresa norte-americana, ele pode fazê-lo em relação às informações que se encontram em sua sede em *Connecticut*, mas estaria proibido, pelas regras da OMC, de obter segredos de empresa do centro de tecnologia da *GE* sediado em *Shangai*. Essa conclusão gera um resultado absurdo na medida em que implica discriminação de proteção fundada simplesmente na posição física e geográfica do segredo, e poderia consistir, inclusive, em uma medida protecionista para a indústria local.

É verdade que o princípio do tratamento nacional, que estabelece que “cada membro concederá aos nacionais dos demais membros tratamento não menos favorável que o outorgado a seus próprios nacionais com relação à proteção” (art. 3 (1) TRIPS), se refere à tutela conferida pela legislação nacional aos direitos de propriedade intelectual nos limites de seu território, e por consequência não se aplicaria à espionagem econômica internacional.³⁶⁴ Todavia, é preciso considerar que os segredos de empresa são protegidos no acordo TRIPS contra práticas de concorrência desleal. Se considerarmos que o Estado-membro que obtém clandestinamente segredo de uma empresa sediada no território de outro Estado-membro irá utilizar as informações para favorecer suas próprias empresas, nota-se uma clara manifestação de deslealdade na concorrência, mesmo se a legislação daquele Estado oferecer um regime de proteção à propriedade intelectual equânime a nacionais e estrangeiros em seu território.

Obviamente, a obtenção clandestina de um segredo de empresa não se converte automaticamente na absorção da inovação e colocação no mercado internacional de um produto ou processo que venha a competir em situação vantajosa sobre concorrentes. Como esclarecem Jon R. Lindsay e Tai Ming Cheung a informação coletada deve ser processada por uma complexa rede de organizações governamentais, transferida para as indústrias e lá convertida com sucesso em um

³⁶⁴ Conclusão contrária foi defendida por Catherine Lotrionte, quando afirmou que: “*It would seem clear, however, that the language of Article III of TRIPS requires as a general obligation under the ‘national treatment principle’ that a country ‘shall accord to the nationals of other members treatment no less favorable than it accords to its own nationals...’ China, in providing government-sponsored commercial intelligence based on stolen IP to its own firms, is giving its own nationals a more favorable treatment, arguably in violation of its obligation under TRIPS*”. LOTRIONTE, Catherine. Countering State-Sponsored Cyber Economic Espionage Under International Law. *North Carolina Journal of International Law and Commercial Regulation*, v. XL, 2015. p. 530.

ganho de performance contra os competidores. Ineficiências ao longo de todo o processo inteligência-inovação pode anular o valor da informação coletada.³⁶⁵

De qualquer forma, uma interpretação do art. 39 do acordo TRIPS que fosse incompatível com o objetivo geral do tratado e outros valores nele enunciados consistiria em uma operação hermenêutica equivocada, de resultado, por consequência, inadmissível. Isso porque, ajustou-se na Convenção de Viena sobre o Direito dos Tratados (1969), em seu art. 31, que “Um tratado deve ser interpretado de boa fé, de acordo com o sentido comum atribuível aos termos do tratado em seu contexto e à luz de seu objetivo e finalidade”. Logo, considerando que a finalidade central do acordo TRIPS, tal como enunciado em seu preâmbulo, é a de “reduzir distorções e obstáculos ao comércio internacional” através de uma “proteção eficaz e adequada dos direitos de propriedade intelectual”, bem como “assegurar que as medidas e procedimentos destinados a fazê-los respeitar não se tornem, por sua vez, obstáculos ao comércio legítimo”, conclui-se que a obtenção clandestina extraterritorial de segredo de empresa é contrária a um sentido maior de proteção à propriedade intelectual que se valoriza no acordo. Ou, nas palavras de Catherine Lotrionte, o acordo TRIPS consagra importantes princípios de honestidade que são inconsistentes com a obtenção extraterritorial de segredo de empresa. Apesar de não existir proibição expressa a atividades de espionagem econômica no acordo TRIPS, tal prática frustra um dos objetivos do acordo e enfraquece compromissos comerciais, devendo ser considerada proibida.³⁶⁶

A verdade é que boa parte da perplexidade diante da questão da espionagem econômica se deve ao fato de ser atividade conduzida remotamente, através do espaço cibernético – o que permite que oficiais do exército chinês posicionados na China obtenham segredos de empresa alocados em servidores no território dos Estados Unidos. Nesse quadro, um conceito de natureza física como o de territorialidade não se adéqua com exatidão aos problemas relacionados à espionagem cibernética; na verdade compromete, inclusive, sua correta

³⁶⁵ “Espionage does not translate simply into innovation, however. Collected data must be processed by a complex network of government and industrial organizations and translated into successful performance against competitors. Inefficiencies throughout the entire intelligence-to-innovation process can erode the value of stolen data”. LINDSAY, J. R.; CHEUNG, T. M. From Exploitation to Innovation... *op. cit.* p. 51-52.

³⁶⁶ “Most importantly, TRIPS enshrines important principles of fair play and honest dealing that are inconsistent with cross-border IP theft for commercial purposes [...] Such theft undermines the purpose of these agreements—to create a fair trade regime among member states”. LOTRIONTE, C. *op. cit.* p. 527.

compreensão. Se considerarmos que o acordo TRIPS foi elaborado em um momento em que não era possível a condução remota de espionagem na mesma dimensão em que o é atualmente, é razoável adaptar a interpretação de seus dispositivos segundo a nova realidade. Compartilhando dessa conclusão, Christina Parajon Skinner afirma:

Se as ações de um Estado-membro tomadas dentro de seu território violam direitos de propriedade intelectual de outro membro, não deveriam as regras da OMC se aplicarem? Que o dano tenha sido causado no espaço cibernético parece uma razão pobre para limitar a aplicação do acordo TRIPS, que foi negociado antes do surgimento das ameaças cibernéticas ao comércio e aos direitos de propriedade intelectual.³⁶⁷

Portanto, conclui-se que a espionagem econômica internacional é uma atividade ilícita, contrária às obrigações de proteção da informação confidencial assumidas através do art. 39 do acordo TRIPS, podendo ser apreciada pelo órgão de solução de controvérsias da OMC se convertida em alguma distorção concorrencial, e inclusive ensejar em outros foros a responsabilidade internacional do Estado que obtém clandestinamente o segredo de empresa.^{368 369}

4.4.4 O argumento da “soberania econômica”

Um outro argumento encontrado na literatura sugere ser ilícita a espionagem econômica internacional por violar o princípio da não-intervenção diante da soberania econômica do Estado alvo da atividade. Argumenta-se que o elemento da coerção, exigível para configuração da intervenção, não se limita ao uso da força e

³⁶⁷ Segundo Christina Skinner: “If a member state’s actions taken from within its territory infringe on another member state’s intellectual property rights, should not the WTO rules apply? That the harm is done in cyber space seems a poor reason to limit application of the TRIPS Agreement, which was, in any event, negotiated before the rise of cyber threats to trade and intellectual property rights”. SKINNER, C. P. *op. cit.* p. 1197. No mesmo sentido, Catherine Lotrionte ao afirmar que “[...] economic espionage, as a highly intrusive coercive act into the economic and political freedoms of a state, may constitute a wrongful act of intervention in violation of the customary norm”. LOTRIONTE, C. *op. cit.* p. 496.

³⁶⁸ O Projeto de Artigos da Comissão de Direito Internacional da ONU sobre Responsabilidade de Estados, um documento cuja autoridade possui amplo reconhecimento doutrinário e jurisprudencial, define, em seu art. 1, que “Todo ato internacionalmente ilícito de um Estado acarreta sua responsabilidade internacional”. UNITED NATIONS. Draft Articles... *op. cit.* Art. 1.

³⁶⁹ Essa assertiva, vale frisar, é feita sob uma ótica puramente legal. Obviamente, a viabilidade política de uma demanda dessa natureza envolve considerações mais complexas de política internacional e política econômica que não são objeto da análise dogmática que se faz nessa seção.

que uma “noção expandida” de soberania derivada do costume internacional inclui a soberania econômica.³⁷⁰

Inicialmente, há, por si só, um problema em se formular conflitos de interesses entre Estados em termos genéricos de “violação da soberania”. Como será discutido na seção 4.5.2.1, a noção de soberania é flutuante, não tem um conteúdo fixo, podendo ser facilmente manipulada pelos Estados para justificar ou condenar determinada ação. Dadas as incertezas e alto grau de generalidade que circundam a noção de soberania, é difícil saber se possui ela uma dimensão que se projete sobre as informações estatais oficiais, o que é agravado pela inexistência de casos apreciados em cortes internacionais sobre a atividade de espionagem internacional de segredos de Estado.

Já a ideia de não-intervenção como consequência da soberania é algo mais concreto, com contornos conceituais mais precisos, o que, no entanto, não a torna isenta de discussões acerca de seu conteúdo. A Carta da ONU não traz uma definição do princípio da não-intervenção, que pode, no entanto, ser inferido como consequência de outros princípios nela homenageados, tais como a igualdade soberana entre os Estados (art. 2, item 1), a proibição geral de ameaça e uso da força (art. 2, item 4) e a limitação da atuação da ONU sobre assuntos que dependam exclusivamente da jurisdição doméstica dos Estados-membros (art. 2, item 7). Relacionados, esses princípios indicam uma proibição de interferência coercitiva em assuntos nos quais outros Estados estão livres para decidir em decorrência de sua soberania, tais como a escolha de seu sistema político, econômico, social e cultural e a condução de sua política externa.³⁷¹

Importante destacar que o elemento coerção é essencial para a configuração da ilicitude da intervenção; segundo a Corte Internacional de Justiça (CIJ), ele “define e, de fato, forma a própria essência da intervenção proibida”.³⁷² No caso de ameaça ou uso da força, em regra proibida em virtude do art. 2 (4) da Carta da

³⁷⁰ “Customary international law also supports an expanded notion of sovereignty, which includes a concept of economic sovereignty that protects private sector actors that contribute to the nation’s economic security. [...] international courts and tribunals have interpreted state sovereignty and the related principles of non-intervention and state responsibility quite broadly, without limiting them to the physical domain”. SKINNER, C. P. *op. cit.* p. 1187-1188.

³⁷¹ INTERNATIONAL COURT OF JUSTICE. **Case Concerning Military and Paramilitary Activities in and Against Nicaragua**, 27 jun 1986. p. 108; UNITED NATIONS GENERAL ASSEMBLY. **Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations**, A/RES/25/2625, 24 out. 1970.

³⁷² INTERNATIONAL COURT OF JUSTICE. **Case Concerning Military...** *op. cit.* p. 108.

ONU³⁷³, a coerção se caracteriza de forma óbvia. O que se questiona é se outras formas de intervenção que não envolvam a utilização da força existem, desde que, é claro, envolvam algum grau de coercitividade. Especificamente no problema que ora se analisa, se há uma dimensão econômica na soberania que justifique o imperativo da não-intervenção em assuntos econômicos.

Tradicionalmente, a ideia de não-intervenção era associada à agressão militar. A própria redação do art. 2 (4) da Carta, ao proibir a ameaça ou uso da força contra “a integridade territorial ou a dependência política de qualquer Estado”, denuncia essa concepção. A esse respeito, é interessante observar que uma proposta de se incluir uma proibição a “medidas econômicas” no art. 2 (4) da Carta da ONU, apresentada pela delegação brasileira na Conferência de São Francisco, foi rejeitada.³⁷⁴

Com o passar dos anos, exigida a aplicação do princípio na apreciação de litígios entre Estados nos foros internacionais, a que correspondeu uma evolução jurisprudencial e doutrinária sobre seu conteúdo, a noção de não-intervenção foi ganhando novos contornos. A Declaração sobre os Princípios de Direito Internacional da Assembleia Geral de 1970 – um documento de interpretação autêntica de reconhecida autoridade – se refere expressamente a aspectos econômicos perante os quais a intervenção é defesa. Afirma-se no texto da Declaração que “todos os Estados tem um direito inalienável de escolher seus sistemas econômico, social e cultural” e que “todas as formas de interferência ou ameaça contra a personalidade do Estado ou contra seus elementos políticos, econômicos e culturais constituem uma violação ao Direito Internacional”.³⁷⁵ Reconhece-se também que “Nenhum Estado pode usar ou encorajar o uso de medidas econômicas, políticas ou de qualquer outro tipo, para coagir outro Estado com o objetivo de obter dele sua subordinação do exercício de seus direitos soberanos e de perceber disso vantagens de qualquer tipo”, texto que vem repetido na Declaração Sobre os Direitos e Deveres Econômicos dos Estados, de 1974.³⁷⁶

³⁷³ O art. 2 (4) da Carta da ONU prevê o princípio de proibição de utilização da força como regra: “Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas”. Excepcionalmente, os Estados poderão utilizar a força quando autorizados pelo Conselho de Segurança (Capítulo VII da Carta) ou em legítima defesa no caso de ocorrência de um ataque armado (art. 51).

³⁷⁴ Cf. SHAW, M. N. *op. cit.* p. 1124, nota de rodapé nº 28.

³⁷⁵ UNITED NATIONS GENERAL ASSEMBLY. **Declaration on...** *op. cit.*

³⁷⁶ *Ibidem*; *Idem*. **Charter of Economic Rights and Duties of States**, art. 32, 1974.

Como se nota da interpretação que se faz sobre o princípio da não-intervenção, há, de fato, uma dimensão econômica da soberania que resguarda o Estado contra medidas que interfiram na escolha e manutenção de seu sistema econômico, especialmente quando isso implique um resultado que diminua sua independência. Exemplos de intervenção econômica nesse sentido incluiriam imposição da escolha de um sistema econômico a outro Estado e embargos e sanções econômicas unilaterais que visam minar o regime de um país visando sua substituição.

Nesses parâmetros, é difícil sustentar que um ato isolado de obtenção clandestina de segredo de empresa conduzida por um Estado contra empresas de outro, ou mesmo um conjunto desses atos, constitua uma violação ao princípio da não-intervenção em sua dimensão econômica. Ainda que se saiba que atos de espionagem econômica possam somar prejuízos bilionários – como os eventos China-Estados Unidos demonstraram – é difícil aferir até que ponto isso representa uma interferência na “soberania econômica” do Estado entendida como sua liberdade de definição de seu sistema e sua independência econômica.

Além do mais, é preciso examinar a presença do requisito da coerção nos atos de espionagem econômica. É verdade que o fato de ser a atividade conduzida através do espaço cibernético não é, por si só, um impeditivo à configuração da coerção.³⁷⁷ É possível conduzir ataques cibernéticos com vírus capazes de destruir redes e sistemas de computadores, como foi o caso do *stuxnet* implantado nas centrífugas de enriquecimento de urânio do Irã (cf. seção 2.1) ou imaginar uma situação em que um Estado manipula notícias na mídia digital em véspera de eleições de outro Estado ou então “derruba” um *site* de determinado partido político.³⁷⁸ Nesses casos se configuraria o elemento “coerção” a ponto de levar a

³⁷⁷ Sobre as peculiaridades do princípio da não-intervenção aplicado ao espaço cibernético, conferir: GILL, Terry D. Non-Intervention in the Cyber Context. In: ZIOLKOWSKI, Katharina. **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy**. NATO Cooperative Cyber Defence Centre of Excellence, Tallin, 2013. p. 217-238.

³⁷⁸ A intrusão de computadores e contas de email ligados ao Comitê Nacional dos Democratas durante a campanha presidencial norte-americana de 2016, de que há fortes indícios de ter sido coordenada pela inteligência russa com a finalidade de interferir no resultado das eleições, seria um bom exemplo de um ato de espionagem que envolva um elemento de coerção. Cf. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. **Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution**, 06 jan. 2017. Disponível em: <<https://assets.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf>>

uma situação de intervenção.³⁷⁹ Não obstante, comenta-se em literatura especializada que a mera intrusão em sistemas de outro Estado não viola o princípio da não intervenção, mesmo se exigir superar *firewalls* ou a “quebra” de senhas.³⁸⁰

Portanto, conclui-se que o argumento da soberania econômica ou não-intervenção em assuntos econômicos não é adequado para apreciação de casos envolvendo espionagem econômica de segredos de empresa. O exame dessas atividades encontra um melhor ponto de referência no contexto da proteção internacional da propriedade intelectual, como discutido na seção anterior.

Conclusão diversa é apresentada por Catherine Lotrionte quando afirma que:

[...] espionagem econômica envolve a subtração de propriedade de entidades de um Estado que resultará em desvantagem para esse Estado no mercado global, afetando negativamente as políticas relacionadas ao comércio internacional. Com frequência, o dano resultante causado pela espionagem econômica irá exigir do Estado vítima alterar suas políticas domésticas e internacionais para conter o dano, **caracterizando assim a espionagem econômica como coercitiva no sentido pretendido pela Corte no caso Nicarágua, e por consequência um ato ilícito de intervenção.**³⁸¹ [g.n.]

O problema desse raciocínio é estar sustentado na premissa de que “o dano resultante causado pela espionagem econômica irá exigir do Estado vítima alterar suas políticas domésticas e internacionais para conter o dano, caracterizando assim a espionagem econômica como coercitiva”. Em primeiro lugar, o fato de a espionagem econômica causar dano pode alçar a responsabilidade internacional do Estado que patrocina a atividade, mas não é, por si só, um elemento de coerção. A coercitividade se expressa pela utilização da força – não apenas militar – de forma contrária à liberdade de escolha do Estado atingido e não pela provocação de um dano, que pode, no entanto, ser uma consequência acidental de um ato de intervenção, não necessário.

³⁷⁹ NORTH ATLANTIC TREATY ORGANIZATION. **Tallin Manual on the International Law Applicable to Cyber Warfare**, Cambridge: Cambridge University Press, 2013. p. 47.

³⁸⁰ “*Mere intrusion into another State’s systems does not violate the non-intervention principle. In the view of the International Group of Experts, this holds true even where such intrusion requires the breaching of protective virtual barriers (e.g., the breaching of firewalls or the cracking of passwords)*”. *Ibidem*. p. 47.

³⁸¹ “[...] *economic espionage involves the theft of property of entities within a state that will disadvantage the state in the global trade market, negatively impacting the state’s policies related to global trade.*”²⁷³ Often, the resulting damage caused by the economic espionage will require the victim state to alter its domestic and international policies to stem the damage, thus making the economic espionage coercive in the manner intended by the Nicaragua Court, and therefore a wrongful act of intervention”. LOTRIONTE, C. *op. cit.* p. 503.

Em segundo lugar não se pode admitir que toda conduta estatal que impelir outro Estado a alterar suas políticas internas e externas para contenção de danos seja caracterizada como intervenção, sob pena de inviabilizar qualquer medida econômica doméstica com alcance global. Pense-se, por exemplo, na decisão do *Federal Reserve System (FED)* em elevar a taxa básica de juros nos Estados Unidos ou a decisão do governo chinês em reduzir a importação de *commodities*. Tratam-se de medidas que possuem impacto direto na economia global e que podem provocar danos significativos a alguns Estados, exigindo que adaptem suas políticas ao novo cenário, mas nem por isso podem ser taxadas como medidas de intervenção coercitiva.

4.5 A discussão sobre a licitude da espionagem de segredos de Estado

Um dos argumentos centrais que vem sendo defendidos neste capítulo é o de que não se pode, do ponto de vista jurídico-dogmático, analisar o fenômeno da espionagem como uma só coisa, algo sobre o que se possa formular um juízo unitário de licitude. De fato, comprovou-se que é prudente analisar a licitude de atos de espionagem de forma compartimentada, em atenção à natureza do titular e da própria informação alvo da coleta.

Entretanto, como já antecipado na abertura do capítulo, muitos autores que se propõem a estudar o *status* jurídico da espionagem ignoram ou desconsideram o fato de que o Direito internacional possui regimes especializados onde se pode encontrar regras específicas que são aplicáveis ao problema da licitude da espionagem internacional. E assim não percebem uma proibição indireta às atividades de espionagem de informações privadas de particulares e de segredos de empresa respectivamente no regime de proteção internacional dos direitos humanos e na proteção internacional da propriedade intelectual, a justificar então uma análise compartimentada da licitude de atos de espionagem.

Esse equívoco, que compromete as próprias premissas da construção do problema, conduz esses comentaristas a formular afirmações sobre uma acepção genérica de espionagem internacional, nas quais se destaca a inexistência de proibição expressa à atividade no Direito Internacional. A transcrição de algumas dessas afirmações irá tornar mais claro o que quer se dizer aqui. Christopher Baker, por exemplo, observa que “o direito internacional não endossa nem proíbe a

espionagem”³⁸²; Roger Scott afirma que “o status da espionagem no direito internacional permanece ambíguo, não especificamente permitido ou proibido”³⁸³; Geoffrey Demarest diz que “O Direito Internacional relativo à espionagem em tempo de paz é virtualmente indefinido, e assim, o direito internacional tem sido uma referência inapropriada e inadequada para tanto a condenação quanto a justificação de ações envolvendo a coleta de informações”.³⁸⁴

Por todo o grupo de autores que constrói sua análise sobre essa noção genérica de espionagem, sem definir qual o tipo de informação a qualificar a atividade cuja licitude se examina, considera-se na tese que tratam eles de espionagem de segredos de Estado – que parece ser mesmo a intenção desses comentaristas – para que assim se proceda à crítica de seus respectivos argumentos.

Por outro lado, se concordam em apontar genericamente uma “lacuna” ou “silêncio” na dimensão positiva do Direito Internacional sobre as atividades de espionagem, a partir daí divergem estes autores a respeito das consequências desse hiato e se separam em três correntes teóricas: a) a que sustenta que a ausência de proibição da espionagem em tratado e costume internacional tem por resultado sua permissividade; b) a que argumenta ser a espionagem permitida por princípios de Direito Internacional e c) a que defende, mesmo diante da inexistência de regras convencionais formais que regulem genericamente a atividade, ser ilícita a espionagem em tempo de paz em atenção a princípios de Direito Internacional.³⁸⁵

Como essas três posições teóricas se iniciam a partir da constatação de um silêncio na dimensão positiva do Direito Internacional sobre a espionagem de

³⁸² “[...] *international law neither endorses nor prohibits espionage*”. BAKER, Christopher D. Tolerance of International Espionage: a Functional Approach. **American University International Law Review**, v. 19, n. 5, 2003. p. 1092.

³⁸³ “[...] *the status of espionage under international law remains ambiguous, not specifically permitted or prohibited*”. SCOTT, R. D. *op. cit.* p. 223.

³⁸⁴ “*International law regarding peacetime espionage is virtually unstated, and thus, international law has been an inappropriate and inadequate reference for either condemnation or justification of actions involving intelligence gathering*”. DEMAREST, G. B. *op. cit.* p. 321.

³⁸⁵ John Radsan enumera ainda uma outra linha de argumentação, a qual ele mesmo se filia, que sustenta que a espionagem não é nem lícita nem ilícita, estando além da regulação do Direito Internacional. Cf. RADSAN, A. J. *op. cit.* p. 602. Mas note-se que estar ou não a espionagem além da regulação do Direito Internacional não é em si uma consideração puramente jurídica de licitude; é algo que diz respeito ao compromisso internacional (*commitment*) e que permeia discussões de política e relações internacionais. Mesmo porque, do ponto de vista técnico-jurídico, uma conduta ou é permitida ou proibida pela lei. A tese abordará essa discussão no capítulo seguinte e o que se objetiva nesse momento é uma análise puramente dogmática.

segredos de Estado, serão elas examinadas à luz de um estudo sobre as lacunas no Direito Internacional.

4.5.1 *A licitude dos atos de espionagem sob a “abordagem Lotus” e o formalismo no Direito Internacional*

Tradicionalmente, imperando uma noção rígida de voluntarismo no Direito Internacional, segundo a qual os Estados estão obrigados a cumprir determinada regra jurídica apenas se e na exata medida em que tenham aceitado livremente a ela se vincular, a existência de direitos e obrigações no Direito Internacional foi verificada através de um procedimento formal de identificação de fontes. Dessa forma, reconhece-se no tratado internacional o mecanismo convencional de criação de regras e, paralelamente, o costume internacional como resultado do desenvolvimento de um padrão de comportamento consistente de Estados, sobre o qual recai um reconhecimento de obrigatoriedade jurídica.

Quando determinada questão – seja ela apreciada por uma corte de forma hipotética por pareceres ou de forma concreta em casos litigiosos – encontra correspondência direta em um tratado ou costume internacional, cria-se uma situação confortável para os intérpretes e aplicadores do Direito, de quem não se exigirá maiores esforços de subsunção. Todavia, é possível que haja situações nas quais o Direito Internacional não oferece resposta imediata a um caso concreto, ou seja, não há tratado ou costume que possa resolver determinado litígio ou mesmo uma situação hipotética de conflito de interesses. Como então um Estado poderá se certificar, por razões de segurança jurídica, de que um determinado ato que almeje realizar é lícito de acordo com o Direito Internacional ou mesmo se ele possui a obrigação de realizá-lo? Como um juiz de uma corte internacional irá decidir uma demanda que recai sobre uma questão litigiosa não solucionável por tratado ou costume internacional?³⁸⁶ Pois note-se que no Direito Internacional, não havendo um órgão legislativo supranacional com poderes para editar regras gerais e abstratas que vinculem os Estados e outros sujeitos, estando assim a criação da norma quase sempre dependente de uma convergência de vontades de seus próprios

³⁸⁶ O recurso aos princípios gerais de Direito e à equidade será analisado mais adiante.

destinatários³⁸⁷, essas situações irão ocorrer com maior frequência se comparadas com ramos domésticos do Direito.

Nessas hipóteses a doutrina reconhece os chamados “casos difíceis”, nos quais não há uma resposta jurídica imediata ou, em termos mais elaborados, a cadeia de argumentos de justificação não é persuasiva a ponto de estabelecer uma concordância entre juristas racionais a respeito de qual solução é a adequada.³⁸⁸

Classicamente, esse tipo de problema foi encarado no Direito Internacional sob um raciocínio formalista de lógica negativa, que flui nos seguintes termos: toda aquela conduta estatal que não fosse proibida por um tratado ou costume internacional seria considerada permitida. Segundo essa visão, o Direito Internacional possuiria natureza proibitiva, isto é, não seria sua tarefa definir competências exatas de atuação do Estado, mas sim estabelecer regras limitando sua liberdade, que existiria *ipso facto*. Logo, esse argumento de evidentes raízes liberais sugere que a esfera de liberdade de atuação legítima do Estado – um reflexo de sua soberania – é ampla na medida em que não é limitada pelo Direito. Aquilo que não for proibido pelo Direito Internacional presumir-se-ia permitido; a ilicitude, por outro lado, não poderia ser objeto de presunção.

Essa forma de conceber a normativa internacional é fruto de longa tradição, que tem sua representação emblemática no caso *S.S. Lotus*, julgado pela Corte Permanente de Justiça Internacional (CPJI) em 1927. A discussão de mérito dizia respeito à colisão em alto-mar entre a embarcação francesa *S.S. Lotus* e a turca *S.S. Boz-Kourt*, da qual resultou a morte de oito nacionais turcos. A Turquia prendeu e reivindicou a prerrogativa de julgar o capitão do *S.S. Lotus*, o senhor Demons, o que foi contestado pela França tendo em vista estar o capitão em embarcação sob pavilhão francês.³⁸⁹ A questão central a ser apreciada pela corte era a de definir se

³⁸⁷ São exceções os costumes internacionais gerais – ainda que se possa dizer que em sua formação há a manifestação indireta da vontade dos Estados na medida em que é possível rejeitar sua vinculação através da chamada “objeção persistente” – as obrigações *erga omnes*, e as normas *jus cogens*.

³⁸⁸ “[...] *conventional doctrine assumes a distinction between “normal” and “hard” cases. The former are those in which the justificatory chain of arguments is experienced (or could rationally be experienced) as persuasive by international lawyers. The latter are those in which reasonable lawyers are left to disagree*”. KOSKENNIEMI, M. **From Apology...** *op. cit.* p. 41.

³⁸⁹ A questão somente viria a ser regulamentada por tratado em 1958, na Convenção sobre o Alto-Mar, que, rejeitando o resultado do caso *Lotus*, determinava em seu art. 11 que: “Em caso de abordagem ou qualquer outro incidente de navegação relativo a um navio no alto mar, de modo a envolver responsabilidade penal ou disciplinar do capitão ou de qualquer outra pessoa ao serviço do navio, nenhum procedimento penal ou disciplinar pode ser intentado contra estas pessoas, a

havia alguma regra de Direito Internacional que proibia um Estado de exercer jurisdição criminal sobre estrangeiro que comete atos fora de sua jurisdição territorial. A conclusão alcançada pela Corte foi a de que não existia tal regra e, portanto, a Turquia não violava o Direito Internacional ao sujeitar o capitão do S.S. *Lotus* a um julgamento criminal, ou seja, estava livre para fazer o que não era proibido pelo Direito Internacional. Nos termos da decisão:

O Direito Internacional governa relações entre Estados Independentes. Dessa forma, as regras de Direito que vinculam os Estados emanam de sua livre vontade tal como expressadas nas convenções ou nos costumes geralmente aceitos como sendo expressões de princípios de direito e estabelecidos com o fim de regular as relações entre essas comunidades independentes coexistentes ou com foco na realização de objetivos comuns. Restrições sobre a independência dos Estados não podem, portanto, ser presumidas.³⁹⁰

Note-se que tal conclusão, que ficou conhecida na doutrina como “princípio Lotus” ou “abordagem Lotus”, toca em duas questões distintas mas relacionadas: lacunas no sistema jurídico e licitude, sendo que a relação estabelecida entre as duas foi a de que a lacuna, isto é, o silêncio do ordenamento jurídico a respeito de determinada conduta estatal, implica sua permissividade. Trata-se de um recurso bastante conveniente para um juiz do ponto de vista pragmático e político: diante de um caso para o qual não há correspondência normativa imediata, ou seja, não há previsão de proibição ou permissividade em tratado ou costume internacional, o julgador evita, ao mesmo tempo, os inconvenientes de declarar o *non liquet* e se

não ser perante as autoridades judiciais ou administrativas, quer do Estado do pavilhão, quer do Estado de que estas pessoas têm a nacionalidade”.

³⁹⁰ “*International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed*”. PERMANENT COURT OF INTERNATIONAL JUSTICE. **Publications of the Permanent Court of International Justice: the case of the S.S. “Lotus”, 1927.** p. 18. Disponível em: <http://www.icj-cij.org/pcij/serie/A/A_10/30_Lotus_Arret.pdf>

recusar a decidir³⁹¹, e, por outro lado, de se investir de poderes legiferantes, estabelecendo uma regra *ad-hoc* para resolver a demanda de forma discricionária.

A doutrina positivista acolheu tal abordagem de forma mais elaborada – ainda que com as mesmas consequências práticas – através do argumento de que o sistema jurídico, na verdade, não possui lacunas. Quando determinada conduta estatal não encontrasse correspondência proibitiva nas regras jurídicas, argumentam os internacionalistas positivistas, isso estaria a significar que o ordenamento jurídico autoriza sua prática, e não de que uma lacuna conduz à sua permissividade. Daí se extrai a ideia de *completude formal do ordenamento jurídico*. Como explicou Hans Kelsen, ao discutir as “chamadas lacunas do Direito” – expressão por ele utilizada:

O Direito Internacional existente pode sempre ser aplicado ao caso concreto, o que significa dizer, à questão de se um Estado (ou outro sujeito de Direito Internacional), está ou não obrigado a se comportar de certa maneira. Se não existe norma de direito convencional ou costume internacional impondo ao Estado (ou outro sujeito de Direito Internacional) a obrigação de se comportar de certa maneira, o sujeito está livre sob o Direito Internacional a se comportar como quiser; e por força desse efeito o Direito Internacional já existente é aplicado ao caso. Mas essa decisão, apesar de logicamente possível, pode não ser moralmente ou politicamente satisfatória. Apenas nesse sentido existem “lacunas” no ordenamento jurídico internacional assim como em qualquer outro.³⁹²

³⁹¹ Mesmo porque, defende-se existir um princípio geral de Direito Internacional de proibição do *non liquet*. Cf. KOSKENNIEMI, M. **From Apology...** *op. cit.* p. 43; LAUTERPACHT, Hersch. Some Observations on the Prohibition of *Non Lique*t and the Completeness of the Legal Order. *Symbolae Verzijl*, 1958. De fato, ainda que nem toda situação possa encontrar a princípio uma regra jurídica correspondente, “every international situation is capable of being determined as a matter of law”. JENNINGS, Robert; WATTS, Arthur [eds.]. **Oppenheim’s International Law**, 9 ed., 1992, p. 13. Note-se que a proibição ao *non liquet* se refere à imprescindibilidade de se proferir uma decisão uma vez conhecido o caso, não impedindo, portanto, que uma corte internacional se recuse a conhecer uma demanda ao argumento de não possuir jurisdição para tanto, ou se recuse a fornecer um parecer sobre determinada questão jurídica, como de fato o fez no caso *Legality of the Use by a State of Nuclear Weapons in Armed Conflict* (1996) diante de um pedido da Organização Mundial da Saúde. Posteriormente, a questão foi apreciada por parecer a pedido da Assembleia Geral da ONU. Cf. INTERNATIONAL COURT OF JUSTICE. **Legality of the threat or use of nuclear weapons**, advisory opinion, 8 july 1996. Disponível em: <<http://www.icj-cij.org/docket/files/95/7495.pdf>>

³⁹² “Existing international law can always be applied to a concrete case, that is to say, to the question as to whether a state (or another subject of international law), is or is not obliged to behave in a certain way. If there is no norm of conventional or customary international law imposing upon the state (or another subject on international law) the obligation to behave in a certain way, the subject is under international law legally free to behave as it pleases; and by a decision to this effect existing international law is applied to the case. But this decision, though logically possible, may be morally or politically not satisfactory. Only in this sense are there ‘gaps’ in the international as in any legal order”. KELSEN, Hans. **Principles of International Law**. Rinehart and Company, 1952. p. 305.

Um recurso teórico arrojado! O modelo kelseniano sugere um ordenamento jurídico fechado, em que sempre se encontra uma resposta correta para qualquer problema legal.³⁹³ O *non liquet*, segundo essa concepção, não seria proibido em razão da existência de um dever judicial de decidir, mas sim porque é logicamente impossível de ocorrer. Isso transmite a ideia de completude formal do ordenamento jurídico mas, como bem observou Gerald Fitzmaurice, “deixa a lacuna material ou substantiva por preencher”³⁹⁴, o que somente se resolveria com a edição de uma norma que viesse a regular a matéria.

Em seguida Kelsen critica duramente a ideia de que, caso a permissividade resultante da ausência de proibição seja moral ou politicamente insatisfatória, possa o juiz criar uma regra aplicável ao caso concreto sob a justificativa de que se está a suprir uma lacuna:

Aquele que assume que nesse caso o Direito existente não possa ser aplicado ignora o princípio fundamental de que o que não é legalmente proibido aos sujeitos de Direito é legalmente permitido a eles. A regra autorizando aos órgãos aplicadores da lei a não aplicar o Direito existente mas a criar novo Direito, no caso da aplicação do Direito existente ser, apesar de lógica, moralmente ou politicamente insatisfatória, confere extraordinário poder legiferante para órgãos de aplicação da lei.³⁹⁵

Ainda assim, Kelsen reconhece que um tratado pode conferir a uma corte internacional o poder de estabelecer normas para suplantiar uma ausência de regulação e, segundo ele, é exatamente o que ocorre com a disposição contida no art. 38, 1(c), do Estatuto da CIJ, que a autoriza a aplicar princípios gerais de Direito para decidir as disputas que lhe foram apresentadas. Nessa situação, os princípios assumiriam a função integrativa como fonte suplementar aos tratados e costumes

³⁹³ Como define Scott Shapiro: “[...] *legal formalism is primarily a descriptive theory about the content of modern legal systems. Roughly put, it claims that in modern regimes there is always a right answer to every legal question, and that it is the responsibility of the judge to find and apply this answer without resorting to moral considerations of any sort*”. SHAPIRO, Scott J. **Legality**. The Belknap Press of Harvard University Press, 2011. p. 240.

³⁹⁴ FITZMAURICE, Gerald. The general principles of international law considered from the standpoint of the rule of law. **Collected Courses of the Hague Academy of International Law**, 1957. p. 55.

³⁹⁵ “He who assumes that in such a case the existing law cannot be applied ignores the fundamental principle that what is not legally forbidden to the subjects of the law is legally permitted to them. The rule authorizing the law-applying organs not to apply existing law but to create new law in case the application of existing law is, though logically possible, morally or politically unsatisfactory, confers an extraordinary lawmaking power upon the law-applying organs”. KELSEN, H. **Principles...** *op. cit.* p. 306.

internacionais.^{396 397} Aparentemente, poderia se identificar aqui um contrassenso no raciocínio de Kelsen pois, não havendo tratado ou costume aplicáveis a determinada questão, como visto, o Estado estaria livre para agir da forma que desejasse. Não haveria que se recorrer a um princípio geral para decidir a questão. Mas note-se que, mesmo nesse caso, a autoridade para aplicar um princípio geral é conferida ela própria por um tratado – no caso o Estatuto da CIJ – e a aplicação do princípio funcionaria como uma cláusula residual de solução de litígios. Além disso, observe-se que não se fala em uma obrigação em aplicar o princípio geral de Direito mas sim em uma faculdade. A solução consistente em reconhecer a liberdade de conduta estatal diante da inexistência de tratado ou costume aplicáveis à questão, mesmo quando se pode recorrer a um princípio geral de Direito, seria igualmente satisfatória no formalismo kelseniano.

Naturalmente, o modelo de ordenamento jurídico internacional de Kelsen está em perfeita consonância com sua Teoria Pura do Direito e as proposições de uma concepção formalista positivista, cuja premissa central é a de que a identificação e aplicação da regra jurídica deve ser feita sem que se recorra a argumentos metajurídicos, especialmente de natureza moral.³⁹⁸ Da mesma forma, as ideias de consentimento e voluntariedade da doutrina internacionalista positivista se encaixam

³⁹⁶ “There can be no doubt that such a power may be conferred upon a law-applying organ by a treaty. It is from this point of view that the provision of Article 38 of the Statute of the International Court of Justice is to be understood: that the Court “whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply” not only conventional and customary international law but also “the general principles of law recognized by civilized nations.” These “general principles of law” are probably supposed to be a supplementary source of international law, to be applied if the two others— treaty and custom—cannot be applied”. KELSEN, H. **Principles**... *op. cit.* p. 307.

³⁹⁷ A posição dominante na doutrina jusinternacionalista, refletida nas decisões da CIJ, é mesmo a de que os princípios gerais de Direito se qualificam como fonte, mas seu escopo de aplicação é limitado, assumindo principalmente a função de auxiliar na interpretação de outras normas ou integrar o ordenamento jurídico em caso de lacunas. Cf. SHAW, M. N. *op. cit.* p. 98. Na verdade, evitar o *non liquet* foi mesmo a razão da inclusão da expressão “princípios gerais” no Estatuto da Corte Permanente de Justiça Internacional. Cf. HUDSON, Manley. **La Cour Permanente de Justice Internationale**. Paris, 1936. p. 618-620. No mesmo sentido: D’ASPREMONT, Jean. **Formalism and the Sources of International Law: a theory of the ascertainment of legal rules**. Oxford University Press, 2011. p. 97 e 171.

³⁹⁸ Essa seria a chamada versão *exclusiva* do positivismo. Uma versão mais moderada, considerada *inclusiva*, admite o recurso a critérios morais na aferição da validade da norma, mas nunca no processo de identificação da norma jurídica. Sobre a distinção entre o positivismo exclusivo e inclusivo conferir SHAPIRO, S. *op. cit.* p. 267 e ss. Observe-se que não se afirma aqui que toda teoria positivista tem caráter formalista ou vice-versa.

coerentemente com o critério Lotus e as proposições formalistas do Direito Internacional como um todo.^{399 400}

Sob essa inspiração, muitos comentaristas do problema da licitude da espionagem internacional atualmente se voltam para a abordagem proposta no remoto caso Lotus para oferecer uma solução. Não encontrando tratado que declare de forma expressa a proibição da espionagem entre Estados, concluem os autores ser a atividade lícita por ausência de proibição.⁴⁰¹ Da mesma forma, não se encontra tal proscrição no costume internacional. Exatamente pela postura não-reflexiva que os Estados sustentam em relação à espionagem, não se pode afirmar que exista uma prática geral de repúdio à atividade se os mesmos Estados que contra ela protestam quando dela se descobrem alvos também a realizam em relação a outros Estados. Não há, portanto, a consistência e a uniformidade necessárias para a configuração de um costume internacional que se revele proibitivo ou permissivo em relação à espionagem. Além disso, o fato de os Estados terem se engajado em atividades de espionagem ao longo da história não autoriza a conclusão de ter disso se derivado a formação de costume internacional. Isso porque, a perfeita configuração dessa fonte exige, além da verificação do elemento objetivo de generalidade da prática, o elemento subjetivo consubstanciado no reconhecimento do Estado de que a adoção de tal prática é obrigatória (*opinio juris*

³⁹⁹ WEIL, Prosper. "The Court Cannot Conclude Definitively...": *non liquet* revisited. **Columbia Journal of Transnational Law**, v. 36, 1997. p. 113.

⁴⁰⁰ De fato, as teses de Hans Kelsen podem ser criticadas por um série de razões, mas incoerência não é uma delas. A propósito, é lamentável a forma como a Teoria Pura do Direito e outras proposições do jurista austríaco são ensinadas no Brasil, através de críticas que partem de leituras equivocadas de suas obras – ou, o que é mais grave, de nenhuma leitura – e que portanto são inválidas já em suas premissas. Sobre isso, vale ler o texto LEAL, Fernando. O Formalista Expiatório: leituras impuras de Kelsen no Brasil. **Revista Direito GV**, v. 10, 2014.

⁴⁰¹ O *Tallin Manual on the International Law Applicable to Cyber Warfare* segue a abordagem Lotus: "International Law is generally prohibitive in nature. Acts that are not forbidden are permitted; absent an express treaty or accepted customary law prohibition, an act is presumptively legal. For instance, international law does not prohibit propaganda, psychological operations, espionage, or mere economic pressure per se". NORTH ATLANTIC TREATY ORGANIZATION. **Tallin Manual**... *op. cit.* p. 52. Observando que "Nowhere in international law is peaceful espionage prohibited", Glenn Sulmasy e John Yoo afirmam que "Intelligence collection has been, and continues to be, necessary for the national security of a nation-state". SULMASY, Glenn; YOO, John. Counterintuitive: Intelligence Operations and International Law. **Michigan Journal of International Law**, v. 28, 2007. p. 628. Ashley Deeks nota que "Several government officials and scholars believe that the Lotus approach provides the best way to think about spying in international law". DEEKS, A. An International Legal... *op. cit.* p. 301. No mesmo sentido, William Banks: "Most scholars maintain that international law either permits cyber espionage or does not regulate it at all. The latter posture is credible in international law because of the Lotus case [...]". BANKS, William C. Cyber Espionage, Surveillance, and International Law: Finding Common Ground. In: **Texas A&M Law Review Symposium**, 17 out. 2014. p. 6. Disponível em: <<http://ssrn.com/abstract=2558155>>

sive *necessitatis*). Comportamentos adotados pelos Estados por qualquer outra razão que não seja a crença de se estar cumprindo com algo obrigatório perante o Direito Internacional, especialmente quando manifestados de forma clandestina, não geram um costume.⁴⁰² No caso da espionagem, sendo a prática, à evidência, adotada por liberalidade e tolerância, não se pode reconhecer em sua reiteração a formação de um costume internacional.⁴⁰³

Ocorre que o argumento liberal da abordagem *Lotus* e, da mesma forma, da proposição positivista kelseniana da completude formal do ordenamento jurídico, ambos tendo como consequência o caráter residual da esfera de liberdade de atuação estatal, encerram dois problemas lógicos e conceituais decisivos. Em primeiro lugar, elucidam a questão da licitude no Direito Internacional em um aspecto puramente teórico e sob uma análise individualizada da conduta de um Estado. Pois, afirmar que um Estado está livre para atuar quando a conduta almejada não esteja proibida por tratado ou costume internacional não ajuda a responder a questão de como solucionar judicialmente uma situação concreta de litígio em que dois ou mais Estados pretendem a realização de condutas em si conflitantes e todas elas não proibidas pelo Direito Internacional. Como destaca Martti Koskenniemi, o formalismo falha ao indicar um critério que permita definir qual dos Estados cuja “liberdade” se dará preferência, criando uma situação de “liberdades conflitantes”.⁴⁰⁴

O problema ocorre na medida em que – outra crítica do internacionalista finlandês – qualquer litígio internacional se torna um “caso difícil” porque os Estados

⁴⁰² Como esclarece Malcolm Shaw, “If one left the definition of custom as state practice then one would be faced with the problem of how to separate international law from principles of morality or social usage. This is because states do not restrict their behaviour to what is legally required. [...] The issue therefore is how to distinguish behavior undertaken because of a law from behavior undertaken because of a whole series of other reasons ranging from goodwill to pique, and from ideological support to political bribery. And if customary law is restricted to the overt acts of states, one cannot solve this problem”. SHAW, M. N. *op. cit.* p. 75.

⁴⁰³ Também identificando a falta do elemento subjetivo para a formação de um costume internacional sobre a espionagem, Pål Wrange afirma que: “In order for a customary norm to be formed, there needs to be not only state practice, but also *opinio juris*, a legal conviction that this practice corresponds to the law. I know of no state that has publicly claimed that espionage in all its forms is legal. On the contrary, states generally deny being involved in illegal espionage, and admit only when there is full proof”. WRANGE, Pål. *Intervention in National and Private Cyber Space and International Law*. In: **The Fourth Biennial Conference of the Asian Society of International Law**, Delhi, 14-16 novembro 2013.

⁴⁰⁴ “Any rule application is capable of being understood as an attempt to delimit the disputing States’ freedoms. To say that “freedom” should be given preference fails singularly to indicate which State’s freedom is meant. This version fails because it is devoid of criteria for preferring between conflicting freedoms”. KOSKENNIEMI, M. **From Apology...** *op. cit.* p. 45-46.

sempre justificam suas ações *prima facie* referindo-se à sua liberdade soberana.⁴⁰⁵

Nesses casos,

[...] o julgador é compelido a fazer uma interpretação da extensão dessa liberdade ou a privilegiar uma soberania sobre a outra de um modo que exige a construção de uma hierarquia de valores para avaliar a ação soberana. A construção dessa hierarquia, no entanto, é necessariamente um caso difícil em um sistema que exclui a presença de uma moralidade natural da perspectiva de quais liberdades poderiam ser avaliadas.⁴⁰⁶

Um segundo problema da doutrina Lotus surge na medida em que, ao partir do princípio da existência de uma esfera de liberdade imanente ao Estado, confere-se ao Direito um caráter limitador, não legitimador da soberania estatal. Ao restringir a função do Direito Internacional a um aspecto proibitivo, além do que há liberdade de atuação, posiciona-se a ideia de liberdade fora do Direito; aquilo que não é tocado pelo Direito se traduz em liberdade de atuação. A liberdade estatal, nesse sentido, não é fruto do Direito mas sim resultado de seu silêncio. Pois note-se que não socorre a concepção formalista dizer que uma conduta cuja prática se diz autorizada pelo Direito por ausência de proibição (liberdade) é equivalente a uma conduta cuja prática seja expressamente autorizada na lei (direito). Isso porque, o exercício de um direito subjetivo é circunscrito e tutelado pela lei e a liberdade, sob a acepção formalista, é o mero “poder agir” por ausência de regulação.⁴⁰⁷ Por consequência dessa tese, condutas estatais conflituosas ou são resolvidas porque o Direito proíbe uma delas por que se opõe ao exercício de um direito subjetivo, ou, na ausência de proibição de ambas, se convertem em “conflito de liberdades” e não podem ser resolvidas pois, por resultarem exatamente do silêncio do Direito, não encontram um critério jurídico correspondente que as solucione.

Os postulados formalistas, mesmo com as consequências problemáticas que implicam, a princípio servem bem para explicar o problema da espionagem

⁴⁰⁵ *Ibidem*. p. 43.

⁴⁰⁶ “In such cases the decision-maker is compelled to make an interpretation of the extent of that liberty or to privilege one sovereign over another in a manner which necessitates the construction of a hierarchy of values for evaluating sovereign action. The construction of such hierarchy, however, is necessarily a hard case in a system which excludes the presence of a natural morality from the perspective of which liberties could be evaluated”. *Ibidem*. p. 43.

⁴⁰⁷ Gerald Fitzmaurice propunha a distinção entre um direito e uma liberdade nos seguintes termos: “A right, jurisprudentially, is something actually accorded, guaranteed or protected; but also defined and circumscribed, by the law – whereas a liberty is simply a freedom of action arising out of the fact that the matter is unregulated by any positive rule”. FITZMAURICE, G. *op. cit.* p. 53.

internacional de segredos de Estado, de fato. Atribuindo a espionagem ao “universo da liberdade de atuação estatal”, diante da inexistência de proibição à atividade no Direito Internacional, formula-se um problema de conflito de liberdades cuja solução demandaria o recurso a um critério que não é imediatamente oferecido. Coerentemente, Estados estão livres para praticar atos de espionagem de segredos de Estado uns contra outros e, por via reflexa, também têm liberdade para conduzir contraespionagem que os anule. Isso traduz bem o real contexto da espionagem internacional. Se, por outro lado, se reconhece que há, não liberdade, mas sim um “direito à espionagem internacional”, deve-se aceitar que um Estado que a realiza se encontra no exercício regular e tutelado de um direito e, por consequência lógica, um terceiro Estado afetado pela atividade deveria quedar inerte diante da prática, não podendo refutá-la mediante a contraespionagem – um resultado absurdo, obviamente.⁴⁰⁸

É verdade, a experiência mostra, que com o passar dos anos, o Direito Internacional – como todo ramo jurídico – evolui, e uma porção maior do universo de condutas e relações estatais possíveis passa a ser objeto de regulamentação, seja por via convencional ou costumeira. Um bom exemplo desse processo evolutivo pode se notar no ajuste de tratados sobre o direito de navegação dos mares, aviação civil e exploração dos corpos celestes.⁴⁰⁹ Em compensação, o incessante progresso científico, econômico e social faz surgir novos espaços das relações humanas e estatais não regulados pelo Direito Internacional, o que ampliaria, por força do formalismo, a esfera de liberdade dos Estados e, por consequência, situações não solucionáveis de exercício de condutas conflitantes não proibidas.

Portanto, o formalismo, como uma teoria descritiva da normativa internacional, de onde se retiram postulados lógicos para a operação de decisão judicial, não fornece um critério para a solução de conflitos de liberdades. A construção de um critério que resolva essas situações, seja por indicar qual das liberdades exercidas

⁴⁰⁸ É preciso dizer que essas ponderações sobre a licitude da espionagem podem sofrer a interferência de algumas variáveis relacionadas à forma como a atividade é conduzida: se envolve ou não intrusão territorial, por exemplo. Isso será discutido na seção 4.5.2.1.

⁴⁰⁹ Respectivamente, poderíamos citar como exemplos desse processo evolutivo o Direito do Mar tradicionalmente regulado por costume internacional e depois positivado nas Convenções de Genebra de 1958 e a Convenção da ONU de 1982 (Montego Bay, Jamaica); A Convenção de Chicago sobre Aviação Civil Internacional de 1946 e o Tratado sobre os Princípios Reguladores das Atividades dos Estados na Exploração e Uso do Espaço Cósmico de 1967.

prevalece ou então por definir seus limites, bem como a inclusão desse critério numa concepção objetiva do direito é o problema central para a teoria formalista.⁴¹⁰

Por outro lado, uma posição inversa à abordagem Lotus significaria afirmar que os Estados somente estão autorizados a realizar aquelas condutas que encontram previsão permissiva em uma regra de Direito internacional. Condutas não regulamentadas presumir-se-iam ilícitas por essa ótica. Esta também não seria uma solução adequada pois iria restringir significativamente as possibilidades de atuação do Estado, principalmente em um cenário político internacional em que a formação de um consenso fosse complexa ou em situações que demandam ações emergenciais que não estão previstas no Direito Internacional. Para o caso específico da espionagem internacional, essa abordagem exigiria reconhecer sua ilicitude por ausência de permissão legal.

4.5.2 *A licitude dos atos de espionagem por aplicação dos princípios gerais de direito*

Se a lógica de aferição da licitude de condutas no formalismo não oferece de imediato um critério que possa solucionar os chamados “conflitos de liberdades”, e o raciocínio inverso é também inadequado por limitar a atuação estatal exageradamente, entre uma e outra forma de resolver o problema da inexistência de regulamentação jurídica a solução mais adequada é, como defendia Gerald Fitzmaurice, a de não estabelecer presunção alguma, seja de licitude ou ilicitude.⁴¹¹ São sugeridos então outros mecanismos de superação das lacunas no ordenamento jurídico.

Uma versão mais moderada que o formalismo Kelseniano também postula a qualidade de completude do ordenamento jurídico mas reconhece, ao contrário daquela, a existência das lacunas. Nesse sentido, o ordenamento jurídico seria completo não por fazer uma presunção de licitude de condutas não regulamentadas, mas sim por conter em si mesmo mecanismos de preenchimento dessas lacunas; seria, sob essa concepção, *materialmente completo* ou, “auto-curativo” nas palavras de Prosper Weil.⁴¹² São basicamente dois estes mecanismos de preenchimento: a

⁴¹⁰ KOSKENNIEMI, M. **From Apology**... *op. cit.* p. 46.

⁴¹¹ FITZMAURICE, G. *op. cit.* p. 51-54.

⁴¹² WEIL, P. *op. cit.* p. 110.

aplicação dos princípios gerais de Direito e o recurso à equidade como método de solução de litígios.

Como se pretende aqui um estudo sobre a licitude das atividades de espionagem de segredos de Estado, as soluções que sugerem a superação da lacuna na dimensão judicial, ou seja, apenas no momento da solução de um litígio, como é o caso do recurso à equidade, não fornecem muitas pistas, pois não são um critério de aferição de licitude *ex ante*. De fato, identificada uma lacuna no ordenamento jurídico, a indeterminância não é resolvida automaticamente pelo recurso à equidade; é necessário que seja ela enfrentada judicialmente. Pendendo a determinação judicial, a lacuna persiste.⁴¹³ Não obstante, é interessante examinar se um eventual litígio que envolva a obtenção clandestina de segredos de Estado pode, ao menos em tese, ser resolvido judicialmente pela equidade, visando, inclusive, complementar o estudo teórico das lacunas que vem sendo feito até este ponto.

A resolução de um litígio com fundamento em uma noção de equidade é autorizada à Corte Internacional de Justiça pelo art. 38 de seu Estatuto, que estabelece a faculdade de se decidir uma questão *ex aequo et bono* se as partes com isso concordarem. De fato, o recurso à equidade, como uma solução construtivista para o litígio, é especialmente relevante nos casos que envolvem o exercício de liberdades sustentadas em uma lacuna jurídica. Foi recorrentemente utilizado pela CIJ em decisões referentes à delimitação territorial: *Anglo-Norwegian Fisheries* (1951), *North Sea Continental Shelf* (1969), *Tunisia-Libya Continental Shelf* (1982), *Gulf of Maine* (1984), entre outros.⁴¹⁴

Um outro bom exemplo de como a equidade se aplica a conflitos de liberdades pode ser visto em situações que demandam a responsabilidade de Estados por atos não proibidos pelo Direito Internacional. Nesses casos, como aponta Koskenniemi, a questão é saber qual é a base para a responsabilidade se não há ilegalidade na conduta danosa.⁴¹⁵ A conclusão alcançada pelos relatores do Projeto da Comissão de Direito Internacional da ONU sobre o assunto é a de que a equidade opera como fonte primária da obrigação nesses casos.⁴¹⁶

⁴¹³ *Ibidem*. p. 112.

⁴¹⁴ Cf. KOSKENNIEMI, M. **From Apology...** *op. cit.* p. 259-263.

⁴¹⁵ *Ibidem*. p. 264.

⁴¹⁶ [...] *the duty to have regard to all interests that may be affected can be seen as arising directly from the obligation to take reasonable care, but it may also be seen as arising out of an equitable principle that supplements and informs the discharge of that obligation. [...] equity operates as a function of the primary rule of obligation, which insists that liability be assessed with reference to*

O fato é que a aplicação da equidade como método de solução de litígios tem se mostrado adequada quando os interesses em conflito podem ser equilibrados por um processo de balanceamento. Em casos de disputas territoriais, determinada demarcação feita por um Estado pode ser contestada por outro, mas não há a ocorrência de um dano irreversível. A natureza dos interesses em jogo exige a mera restauração de um equilíbrio. No caso da espionagem de segredos de Estado, diversamente, a obtenção de uma informação classificada normalmente conduz a um prejuízo estratégico material para seu titular. Uma vez conhecido um segredo de Estado não há como restaurar o *status quo ante*, nem mesmo readequar os interesses em disputa para fazer retornar o equilíbrio entre as partes. Por essa razão, a natureza de uma eventual demanda que envolva a espionagem de segredos de Estado não é adequada a uma solução via equidade.

Por sua vez, a análise dos princípios gerais de Direito permite o exame da licitude da espionagem de segredos de Estado em uma dimensão abstrata, e sua aplicação é um recurso válido se não se quer admitir as premissas da abordagem Lotus e reconhecer automaticamente a licitude da atividade. De fato, ao se identificar no ordenamento jurídico valores nucleares estruturantes, subjacentes às próprias regras, o julgador pode neles retirar uma solução para determinada questão não regulamentada por tratado e sem correspondência no costume internacional, evitando assim o *non liquet* ou as premissas do formalismo.

Esses valores normalmente se relacionam com ambições naturalísticas de justiça substantiva como igualdade e coexistência pacífica dos povos, dignidade da pessoa humana e boa-fé ou, em uma dimensão mais pragmática, soberania e não-intervenção, *pacta sunt servanda*, responsabilidade internacional e coisa julgada. Como observa Malcolm Shaw, as decisões das cortes internacionais não deixam claro, em todas as situações, se o que está envolvido é um princípio geral de Direito ou um princípio geral de Direito Internacional, o que não deve, no entanto, ser encarado como um problema sério uma vez que tanto os conceitos jurídicos domésticos quanto aqueles derivados da prática internacional podem ser

the injurious consequences suffered by the innocent victim as well as with reference to the quality of the act". Cf. UNITED NATIONS. Preliminary report on International liability for injurious consequences arising out of acts not prohibited by international law, **International Law Commission**, 1980. p. 260-261. Disponível em: <http://legal.un.org/docs/?path=../ilc/documentation/english/a_cn4_334.pdf&lang=EFS> Conferir também KOSKENNIEMI, M. **From Apology...** *op. cit.* p. 264, nota de rodapé nº 149.

reconhecidos.⁴¹⁷ Dessa forma, é possível que estes princípios estejam previstos nos ordenamentos jurídicos internos ou, internacionalmente, em tratados – o que reforça o reconhecimento de sua obrigatoriedade – ou, em não o sendo, sua existência pode ser em resoluções da Assembleia Geral da ONU e nas decisões judiciais em que são identificados e interpretados.

Além de servirem de mecanismo de preenchimento de lacunas, reconhece-se que os princípios gerais de Direito possuem importante função hermenêutica, na medida em que, ao enunciar valores genéricos, podem orientar a interpretação de outras normas de incidência mais específica. Sob a inspiração de que são expressões do ideal de Direito e de justiça e “refletem a consciência da humanidade”, Antônio Augusto Cançado Trindade defende que os princípios gerais de Direito se posicionam em um nível superior às normas de Direito Internacional Positivo.⁴¹⁸ Ora, a par dos problemas em se saber se existe realmente algo como “consciência da humanidade” ou as diferentes visões que cada sociedade tem sobre justiça, o problema do raciocínio do autor reside na hierarquização dos princípios com base em sua pretensa superioridade axiológica.⁴¹⁹ Pois a distinção de natureza entre os princípios e tratados é apenas de forma e grau de especificação: os princípios gerais de Direito enunciam valores genéricos, em uma dimensão mais ampla e abstrata à especificação escrita de obrigações através dos tratados.⁴²⁰ Não por outra razão, um tratado pode revogar um princípio.⁴²¹

⁴¹⁷ “It is not clear, however, in all cases, whether what is involved is a general principle of law appearing in municipal systems or a general principle of international law. But perhaps this is not a terribly serious problem since both municipal legal concepts and those derived from existing international practice can be defined as falling within the recognised catchment area” SHAW, M. N. *op. cit.* p. 99.

⁴¹⁸ “As basic pillars of the international legal system (as of any legal system), those principles give expression to the *idée de droit*, and furthermore to the *idée de justice*, reflecting the conscience of humankind. Irrespective of the distinct approaches to them, those principles stand ineluctably at a superior level to the norms or rules of positive international law. Such rules and norms are binding, but it is the principles which guide them”. TRINDADE, Antônio Augusto Cançado. *International Law for Humankind: Towards a New Jus Gentium. Collected Courses of the Hague Academy of International Law*, parte II, 2005. p. 96-97.

⁴¹⁹ Em outra passagem do texto o autor afirma: “It is the general principles of law (*prima principia*) which confer on the legal order (both national and international) its ineluctable axiological dimension”. *Ibidem.* p. 86.

⁴²⁰ Como reconhecido, aparentemente de forma contraditória, pelo próprio Cançado Trindade, quando afirma: “Principles of International Law are guiding principles of general content, and in that they differ from the norms or rules of positive International Law”. *Ibidem.* p. 96.

⁴²¹ Há quem defenda uma posição ainda mais radical, afirmando que no caso de conflito entre um princípio geral de Direito e um tratado ou costume, os últimos prevalecem: “Since the main function of general principles of law is to fill gaps in treaty law and customary law, it would appear that general principles of law are subordinate to treaties and custom (that is, treaties and custom

No plano da aplicação, a distinção entre princípios e regras – ao menos em uma abordagem pós-positivista do Direito – também não se relaciona com considerações axiológicas, mas sim lógicas.⁴²² As regras são *comandos definitivos* (Robert Alexy), à maneira “tudo ou nada” (Ronald Dworkin): ou se verifica uma hipótese fática para sua aplicação, quando há a *subsunção* da regra ao fato, ou não há aplicação. Exemplificativamente, a regra que estipula a aplicação de multa ao condutor de veículo automotor que ultrapassa o sinal vermelho, ou se aplica na ocorrência concreta dessa hipótese ou não interfere na situação. Conflitos entre regras – situações em que duas ou mais regras aparentemente se aplicam à determinado fato – se resolvem por recurso à critérios de solução de antinomia⁴²³, e apenas uma das regras envolvidas será aplicada, sendo a outra ou as demais excluídas. Os princípios, por outro lado, são *comandos de otimização* (Alexy), que podem ser aplicados em graus, segundo as possibilidades fáticas e jurídicas do caso. Assim, tome-se como exemplo o princípio de proteção à saúde em confronto com o princípio da liberdade do exercício do comércio no caso específico da venda de cigarros. O princípio de proteção à saúde pode ser aplicado de forma a provocar níveis diferentes de intervenção sobre a liberdade de comércio. Se for realizado em grau máximo, poderia implicar a proibição total da comercialização de cigarros para determinada empresa; em grau médio, a restrição da comercialização do produto em locais frequentados por crianças e, em grau mínimo, a obrigação de veicular nas embalagens de cigarro referências aos riscos que o consumo do produto acarreta para a saúde.⁴²⁴ Por força desse efeito gradativo, conflitos entre princípios são resolvidos por *ponderação*, de forma que dois ou mais princípios podem ser concomitantemente aplicados ao mesmo caso sem que seja necessário excluir algum deles.

Portanto, é perfeitamente adequado e desejável que se reconheça a importância da dimensão principiológica do Direito como espaço orientador da

prevail over general principles of law in the event of conflict). MALANCZUK, Peter. **Akerhurst's Modern Introduction to International Law**, 7 ed., 2002. p. 56.

⁴²² Sobre a distinção entre regras e princípios em uma concepção pós-positivista, conferir: DWORKIN, Ronald. **Levando os Direitos a Sério**. Tradução: Nelson Boeira. 1 ed. Martins Fontes, 2002. p. 35-46; ALEXY, Robert. **The Argument From Injustice: A Reply to Legal Positivism**. Tradução de Stanley L. Paulson e Bonnie Litschewski Paulson. Oxford University Press, 2002. p. 70 e ALEXY, Robert. **Constitucionalismo Discursivo**. Tradução: Luís Afonso Heck. 3 ed., 2011. p. 131-137.

⁴²³ “Regra posterior revoga regra anterior”; “regra especial revoga regra geral” e “regra superior revoga regra inferior”.

⁴²⁴ O exemplo foi adaptado de ALEXY, R. **Constitucionalismo...** *op. cit.* p. 133-134.

criação e aplicação de regras jurídicas; mas que se atribua aos princípios não positivados uma relevância superior às normas convencionais expressas parece algo exagerado. De fato, a aplicação dos princípios gerais tem se mostrado limitada na experiência dos tribunais internacionais⁴²⁵, ao menos no que diz respeito a princípios não positivados em tratados. É normal ver juízes de cortes internacionais fazerem menção a princípios *obiter dicta*, ou seja, na fundamentação de suas decisões, mas dificilmente concluem decisivamente uma controvérsia com base tão somente em um princípio geral de Direito. Mesmo porque, por razões políticas, a CIJ prefere reconhecer a existência de obrigações aos Estados que foram expressamente contraídas por eles. O recurso exclusivo a valores gerais e abstratos poderia desmotivar os Estados a submeterem suas controvérsias ao procedimento judicial da Corte e assim levá-los a recorrer a outros meios de solução como, por exemplo, a arbitragem.

4.5.2.1 O argumento da ilicitude da espionagem pelo princípio da soberania e dos princípios corolários da não-intervenção e da integridade territorial

Um grupo de comentaristas do problema da licitude da espionagem internacional – que serão mencionados ao longo dessa seção – rejeita a abordagem Lotus e, mesmo reconhecendo a inexistência de proibição expressa à atividade, argumenta ser sua prática contrária aos princípios da soberania e seus corolários da não-intervenção e da integridade territorial e, portanto, proscria pelo Direito Internacional.

Inicialmente é preciso observar que sempre há um alto grau de generalidade e incerteza que envolve a própria noção de soberania estatal. Ainda que se possa identificar qualidades e consequências que circundam a ideia de soberania, uma definição conceitual precisa desse instituto é extremamente difícil de se elaborar⁴²⁶, outros diriam teoricamente inadequada.⁴²⁷

⁴²⁵ Como afirma Malcom Shaw: “[...] *most writers are prepared to accept that the general principles do constitute a separate source of law but of fairly limited scope, and this is reflected in the decisions of the Permanent Court of International Justice and the International Court of Justice*”. SHAW, M. N. *op. cit.* p. 99.

⁴²⁶ Como observou Alf Ross, sobre o tema “soberania”, “[...] *there is hardly any domain in which the obscurity and confusion are as great as here. It is not only that there are almost as many definitions of the term ‘sovereignty’ as there authors, but also that there is no agreement as to what purpose is served by this concept in International Law*”. ROSS, Alf. **A Textbook of International Law**.

Além disso, como observa Martti Koskenniemi, a doutrina moderna da soberania sofre de ambiguidades decorrentes de um paradoxo: de um lado, não é possível definir os limites da soberania estatal de forma unitária e isolada em relação a um Estado. É preciso investigar as formas de que essa soberania se relaciona com outras, ou seja, o contexto social em que está inserida, pois é exatamente através da violação da soberania de um Estado que se identifica o limite do exercício das liberdades de outro. Em outros termos, a esfera de liberdade de um Estado deve ser delimitada pelas esferas de liberdade dos demais Estados. Logo, a fim de identificar quais são os exatos limites do domínio de liberdade de atuação de um Estado, não se pode recorrer à própria definição que ele propõe – isto é, aquilo que ele acredita ser a extensão de sua soberania – pois, assim sendo, com frequência o exercício de liberdades estatais se conflitariam em uma zona de confusão, em que dois ou mais Estados acreditam poder agir em decorrência dos diferentes limites a que confiam estar sujeitos. Essa seria uma solução de *apologia*, como caracterizaria Koskenniemi. Logo, os critérios de definição da liberdade estatal devem ser buscados em uma perspectiva externa ao Estado. Por outro lado – aqui reside o paradoxo – não se pode derivar os limites da liberdade estatal completamente das suas relações com outros Estados, em uma perspectiva normativa externa e superior que não considere a vontade do Estado, sem com isso prejudicar sua individualidade como uma nação independente. Seria uma solução *utópica*.⁴²⁸

Portanto, não havendo um conteúdo predeterminado de soberania que especifique seus limites e as condições em que é violada, qualquer Estado irá manipular seu conceito, restringindo-o ou ampliando-o segundo queira justificar a legitimidade de uma ação sua que interfira na esfera de liberdade de outro Estado ou repudiar uma ação alheia que produza efeitos indesejáveis na sua própria esfera

Longmans, 1947. p. 34. No mesmo tom pessimista, Michael Akehurst afirmou, em obra atualizada por Peter Malanczuk, que: “[...] *it is doubtful whether any single word has ever caused so much intellectual confusion and international lawlessness*”. MALANCZUK, P. *op. cit.* p. 17. Por fim, ainda sobre a dificuldade de conceituação do instituto, merece destaque a observação de Carl Schmitt: “*Of all juristic concepts the concept of sovereignty is the one most governed by actual interests*”. SCHMITT, Carl. Tradução: George Schwab. **Political Theology**: Four Chapters on the Concept of Sovereignty. Chicago: University of Chicago Press, 1985. p. 16.

⁴²⁷ Martti Kosekenniemi, por exemplo, sustenta que: “*The expression ‘sovereignty’ or any definition thereof cannot have such fixed content as to be ‘automatically’ applicable. It is not only that they are ambiguous or have a penumbra of uncertainty about them. There simply is no fixed meaning, no natural extent to sovereignty at all*”. KOSKENNIEMI, M. **From Apology**... *op. cit.* p. 242.

⁴²⁸ KOSKENNIEMI, M. **From Apology**... *op. cit.* p. 225.

de liberdade. Nesse sentido já se disse que a soberania nada mais é que “hipocrisia organizada”.⁴²⁹

Dessa forma, entre a apologia e a utopia:

Frequentemente, ambas as partes em uma disputa formulam suas alegações nos termos de sua soberania. Para resolver tais disputas, a doutrina é forçada a olhar além da simples descrição do poder soberano, nas normas que preveem ou delimitam tal poder. Mas de forma a ser justificável, estas normas devem remontar às soberanias elas próprias. E disso emerge o problema de como elas podem ser usadas para alcançar tal delimitação.⁴³⁰

Como se nota, a soberania não pode ser então ela própria uma norma de delimitação do poder. Pelo contrário, ela é o objeto da delimitação normativa. Mas se o fundamento para a obrigatoriedade dessas normas reside justamente no consentimento do poder soberano, então cria-se uma armadilha cíclica. Essa constatação é o ponto de partida de uma sólida crítica ao princípio do consentimento no Direito Internacional que extrapola o objeto da presente análise, mas a que se remete o leitor pelo interesse que desperta no estudo da Teoria do Direito Internacional.⁴³¹

Tudo isso não significa que a noção de soberania deva ser completamente abandonada mas apenas repensada, ao menos em sua dimensão conceitual. De fato, o vocabulário utilizado para explicar sua noção sempre parece insuficiente para capturar seu exato significado. “É como se houvesse algum excesso na soberania que resistisse se conter em um único vocabulário técnico”.⁴³² Por essa razão, observou Jan Klabbers, que

⁴²⁹ A expressão é de Stephen Krasner, quem faz incisiva crítica à manipulabilidade do conceito de soberania em: KRASNER, Stephen D. **Sovereignty**: organized hypocrisy. Princeton University Press, 1999.

⁴³⁰ “*The former is expressed in the manner in which recourse to ‘sovereignty’ seems always available, in one form or another, to legitimize what first appear like clear breaches of the State’s international obligations. Not infrequently both parties in a dispute put their conflicting claims in terms of their sovereignty. To solve such disputes, doctrine is forced to look beyond any simple description of sovereign power into the norms which convey or delimit such power. But in order to be justifiable, these latter norms will have to be traced back to the sovereigns themselves. And from this emerges the problem of how they can be used to achieve such delimitations*”. KOSKENNIEMI, M. **From Apology...** *op. cit.* p. 225-226.

⁴³¹ Conferir, por exemplo, a crítica feita em DWORKIN, Ronald. A New Philosophy for International Law. **Philosophy and Public Affairs**, v. 41, n. 1, 2013.

⁴³² KOSKENNIEMI, Martti. Conclusion: vocabularies of sovereignty – powers of a paradox. In: KALMO, Hent; SKINNER, Quentin. **Sovereignty in Fragments**: the past, present and future of a contested concept. Cambridge University Press, 2010. p. 223.

[...] há uma certa tendência para acabar com a noção totalmente (ao menos no nível semântico) ou, alternativamente, reconceitualizá-la de forma a assegurar que não mais funcione como um mecanismo fundamental ordenador, mas apenas como um conjunto de prescrições relacionadas de não-intervenção.⁴³³

De qualquer forma, não sendo a noção genérica de soberania um critério apto a definir, por si só, o limite da liberdade de atuação estatal, ela pode flutuar para caracterizar como lícita ou ilícita a espionagem internacional dos segredos de Estado, notadamente quando não existe em paralelo uma norma que expressamente faça essa definição. Pois, qual aspecto da soberania seria violado quando um Estado obtivesse clandestinamente uma informação sigilosa de outro? Existe uma dimensão da soberania que se projete sobre as informações estatais oficiais? Existe um direito ao segredo no Direito Internacional?

Essas questões, na forma como estão formuladas, são extremamente difíceis de responder em razão da inexistência de contenciosos envolvendo espionagem de segredos de Estado nas cortes internacionais – outro sintoma da tolerância jurídico-política da atividade. O mais próximo que disso já se chegou – ainda assim de forma remota – foi no caso “*Questions relating to the Seizure and Detention of Certain Documents and Data*” (2013), envolvendo o Timor-Leste e a Austrália. A demanda foi iniciada junto à CIJ pelo Timor-Leste após oficiais da Organização Australiana de Inteligência e Segurança, agindo sob a autoridade de um mandado expedido pelo Procurador-Geral da Austrália, terem adentrado a residência do conselheiro jurídico do Timor-Leste lotado em Camberra e dali apreendido documentos oficiais classificados de propriedade deste país.⁴³⁴

Apesar de se tratar da obtenção de informações classificadas de um governo por outro, o caso, bastante peculiar, fornece poucas pistas para o estudo da licitude da espionagem de segredos de Estado. Evidentemente, não se trata de uma atividade de espionagem internacional pois os documentos foram apreendidos em território da Austrália – nem sequer em uma embaixada – através de um procedimento de busca e apreensão, o que indica a seu titular a detenção da

⁴³³ “[...] there is a certain tendency to do away with the notion altogether (at least on the level of semantics) or, alternatively, to re-conceptualize it in such a way as to ensure it no longer functions as a fundamental ordering mechanism, but merely as a set of related non-intervention prescriptions”. KLABBERS, Jan. Clinching the concept of sovereignty: Wimbledon redux. **Austrian Review of International and European Law**, v. 3, 1998.

⁴³⁴ INTERNATIONAL COURT OF JUSTICE. **Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia)**, Application, 17 dez. 2013. p. 2. Disponível em: <<http://www.icj-cij.org/docket/files/156/17962.pdf>>

informação pelo governo estrangeiro. Além disso, o governo do Timor-Leste fundamentou sua pretensão no direito de propriedade física sobre os documentos, reivindicando o retorno da posse e a destruição de eventuais cópias, e não sobre o dano decorrente da violação da confidencialidade dos documentos.⁴³⁵ Não bastasse, a diminuir a contribuição do caso para o estudo da licitude da espionagem de segredos de Estado, o contencioso não alcançou um julgamento de mérito pois antes o Timor-Leste desistiu da demanda, uma vez que a Austrália devolveu os documentos apreendidos. Ainda assim, no curso do processo, em decisão favorável à aplicação de medidas provisionais – dentre elas o selamento dos documentos apreendidos até decisão final – reconheceu-se que existe um “plausível direito” de confidencialidade e não-interferência sobre as comunicações que um Estado mantém com seu conselheiro jurídico, ao menos no contexto de negociações de acordos internacionais ou procedimentos arbitrais, que era a finalidade do aconselhamento jurídico na hipótese e do que se tratava o conteúdo dos documentos apreendidos.⁴³⁶

A carência de referência na jurisprudência internacional, portanto, torna difícil saber até que ponto uma noção genérica de soberania se estende às informações sigilosas de um Estado. Observe-se ainda que, mesmo se tomarmos a noção de soberania sob uma acepção mais restrita e concreta de não-intervenção, ainda assim é problemático sustentar que a espionagem de segredos de Estado é uma atividade contrária ao Direito Internacional. Como discutido na seção 4.4.4, se a atividade que se pretenda caracterizar como intervencionista não for revestida de algum grau de coercitividade, não há que se falar em violação do princípio da não-intervenção. Com efeito, como cristalizado na jurisprudência da CIJ, o elemento coerção é essencial para a configuração da ilicitude da intervenção; ele “define e, de fato, forma a própria essência da intervenção proibida”.⁴³⁷ Como a espionagem, por definição conceitual, se restringe apenas à obtenção clandestina da informação, não

⁴³⁵ “Timor-Leste asserts that the bulk of the items seized are actually and in law the property of Timor-Leste and that no third party, e.g. the Australian Government, has any rights to or in respect of them. Timor-Leste is entitled to confidentiality in respect of all of these materials [...]” INTERNATIONAL COURT OF JUSTICE. **Questions Relating...** *op. cit.* Memorial of the Democratic Republic of Timor-Leste, 28 abr. 2014. p. 26.

⁴³⁶ “Accordingly, the Court considers that at least some of the rights for which Timor-Leste seeks protection — namely, the right to conduct arbitration proceedings or negotiations without interference by Australia, including the right of confidentiality of and non-interference in its communications with its legal advisers — are plausible”. INTERNATIONAL COURT OF JUSTICE. **Questions Relating...** Application and Request for the indication of provisional measures, 3 mar. 2014. p. 3.

⁴³⁷ INTERNATIONAL COURT OF JUSTICE. **Case Concerning Military...** *op. cit.* p. 108.

há, na essência da atividade, qualquer coerção envolvida. O que pode ocorrer é que o meio através do qual a espionagem é viabilizada pode se revestir de coercitividade e, por consequência, de ilicitude, como é o caso da intrusão territorial que precede a espionagem. Ainda assim, é preciso notar, como será melhor detalhado adiante, que a espionagem e a atividade que a viabiliza são práticas que ocorrem em momentos distintos, e devem ter sua licitude apreciada de forma separada.

Por fim, se compreendermos a soberania em sua acepção territorial, é possível formular um argumento mais plausível de que a espionagem é algo contrário ao Direito Internacional. Esse argumento foi defendido por Quincy Wright nos seguintes termos:

Em tempo de paz, entretanto, a espionagem e, na verdade, qualquer penetração no território de um Estado por agentes de outro Estado em violação à lei local, é também uma violação da regra de Direito Internacional que impõe um dever aos Estados de respeitar a integridade territorial e independência política de outros Estados.⁴³⁸

A regra a que se refere Quincy Wright é o art. 2 (4) da Carta da ONU, que determina que:

Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas.

Como se nota, o princípio da integridade territorial é algo tutelado na Carta de forma simbiótica com a proscrição genérica da utilização da força. A ideia que transmite o dispositivo, portanto, é a de que um Estado não pode usar da força para empreender campanhas de aquisição de território alheio, que tem assim sua integridade protegida. Não obstante, argumenta-se que o aludido princípio merece interpretação extensiva de forma a cobrir situações de entrada não-autorizada de

⁴³⁸ “In time of peace, however, espionage and, in fact, any penetration of the territory of a state by agents of another state in violation of the local law, is also a violation of the rule of international law imposing a duty upon states to respect the territorial integrity and political independence of other states”. WRIGHT, Q. *op. cit.* In: STANGER, R. *op. cit.* p. 12. No mesmo sentido, a afirmação de John Kish: “The general principle of exclusive sovereignty over national territory is firmly established in customary international law. Each state exercises control over its national territory to the exclusion of all other States, and any limitation of this authority is subject to the consent of the territorial State. In particular, no State is entitled to carry out strategic observation in the national territory of another state State without specific agreement”. KISH, John. *International Law and Espionage*. **Martinus Nijhoff Publishers**, 1995. p. 83.

agentes estatais em território estrangeiro.⁴³⁹ Nesse sentido, a espionagem que envolvesse intrusão territorial por agentes estrangeiros consistiria em uma violação ao princípio da integridade territorial e seria ilícita de acordo com o Direito Internacional.

É preciso ter em mente, todavia, que o que se busca examinar é a licitude da espionagem por si só perante o Direito Internacional, vale dizer, com atenção apenas à obtenção clandestina da informação classificada. A forma como é conduzida a espionagem, seja através de intrusão territorial aérea ou terrestre, seja por meio cibernético ou mesmo através de satélites de reconhecimento, entre várias outras modalidades, deverá ter sua licitude apreciada autonomamente, não se confundindo com a licitude da obtenção da informação em si. trata-se do que Julius Stone, ao ponderar sobre essa distinção, denominou de “ilegalidade colateral”⁴⁴⁰ (*rectius*, “ilicitude colateral”). De fato, o que é ilícito nas hipóteses de intrusão territorial não é propriamente o ato de coleta da informação sigilosa, mas sim o meio através do qual ela é viabilizada. São momentos separados: se um avião militar invade o espaço aéreo de um Estado para fins de coleta de informações sigilosas (ex: localização de uma base de lançamento de mísseis), a violação do Direito Internacional se dá no momento em que há a intrusão no espaço aéreo, de sorte que a obtenção da informação pode nem mesmo ser alcançada posteriormente.⁴⁴¹

⁴³⁹ Compartilhando esse posicionamento, Ashley Deeks ao afirmar que: “*Respect for territorial integrity is generally construed to mean that force should not be used to alter interstate boundaries. But it also means that one state may not enter another state’s territory, airspace, or territorial waters without the latter’s consent*”. DEEKS, A. An International Legal... *op. cit.* p. 304. Igualmente, Simon Chesterman quando diz: “*The foundational rules of sovereignty, however, provide some guidance on what restrictions, if any, might be placed on different forms of intelligence gathering that do not rise to the level of an armed attack or violate other specific norms [...] This would clearly cover unauthorized entry into territory; it would also cover unauthorized use of territory, such as Italian claims that CIA agents abducted an Egyptian cleric in Milan in February 2003 in order to send him to Egypt for questioning regarding alleged terrorist activities, as well as the use of airspace to transfer such persons as part of a program of “extraordinary renditions.”*” CHESTERMAN, S. *op. cit.* p. 1081-1082.

⁴⁴⁰ STONE, J. Legal Problems of Espionage in Conditions of Modern Conflict. *In*: STANGER, R. *op. cit.* p. 34. O autor, já na década de 1960, bem observou a tendência que faria com que, no futuro, técnicas de espionagem se aprimorassem e fossem cada vez mais realizadas sem necessidade de intrusão territorial e, portanto, não acarretariam qualquer tipo de ilicitude colateral.

⁴⁴¹ Foi precisamente isso o que aconteceu no caso do abatimento do avião de reconhecimento estadunidense U-2 em sobrevoo na União Soviética em 1960. O episódio resultou na captura do piloto Francis Gary Powers – quem ficou sob custódia da União Soviética até uma troca de prisioneiros realizada em 1962 – e no cancelamento da Cúpula de Paris, onde se reuniriam, com a perspectiva de celebração de um acordo para por fim à crise, os chamados “*Big Four*” (O presidente norte-americano Dwight Eisenhower, o líder soviético Nikita Khrushchev, o general francês Charles de Gaulle, e o primeiro-ministro britânico Harold Macmillan).

Além disso, é possível que a entrada de um agente estatal com ordens para o exercício da espionagem em território estrangeiro se dê de forma lícita, através do corpo diplomático do Estado acreditante – que é mesmo a forma mais comum de ingresso de oficiais de inteligência em outros Estados. Caso o oficial de inteligência ou o diplomata venha a empreender atividades de espionagem, se imiscuindo em assuntos internos do Estado acreditado e violando suas leis – o que é proibido pelo art. 41 da Convenção de Viena sobre Relações Diplomáticas – o fazendo encorajado pela imunidade de jurisdição penal que lhe acoberta, poderá ser declarado *persona non grata* e dele ser expulso por ter excedido em suas atribuições e engajado em práticas incompatíveis com a diplomacia (art. 9).⁴⁴² Por via reflexa, a espionagem que tenha por alvo as comunicações diplomáticas devem ser consideradas ilícitas segundo o Direito Internacional por violação às garantias de inviolabilidade dos arquivos e documentos da missão (art. 24), e dos documentos e correspondências do agente diplomático (art. 30, item 2).

Uma outra hipótese de espionagem praticada via intrusão territorial é a realizada por embarcações que exercem o direito de passagem inofensiva em águas territoriais estrangeiras.⁴⁴³ A Convenção das Nações Unidas sobre o Direito do Mar garante o direito de passagem inofensiva (art. 17) e regulamenta seu exercício em seu art. 19(2) que dispõe que “A passagem de um navio estrangeiro será considerada prejudicial à paz, à boa ordem ou à segurança do Estado costeiro, se esse navio realizar, no mar territorial [...]: c) Qualquer ato destinado a obter informações em prejuízo da defesa ou da segurança do Estado costeiro; [...] l) Qualquer outra atividade que não esteja diretamente relacionada com a passagem. Nessas condições, pode-se concluir que a espionagem internacional praticada em águas territoriais, superficiais ou submarinas, é ilícita perante o Direito Internacional.

Um argumento sustentado por James Kraska sugere que a embarcação que realiza espionagem em águas territoriais no exercício do direito de passagem

⁴⁴² Determina o art. 9 da Convenção de Viena sobre as Relações Diplomáticas: “O Estado acreditado poderá a qualquer momento, e sem ser obrigado a justificar a sua decisão, notificar ao Estado acreditante que o Chefe da Missão ou qualquer membro do pessoal diplomático da Missão é *persona non grata* ou que outro membro do pessoal da Missão não é aceitável. O Estado acreditante, conforme o caso, retirará a pessoa em questão ou dará por terminadas as suas funções na Missão. Uma Pessoa poderá ser declarada *non grata* ou não aceitável mesmo antes de chegar ao território do Estado acreditado”.

⁴⁴³ Vale a observação de que o direito de passagem inocente também pode ser exercido através de submarinos, desde que feita na superfície e com a bandeira hasteada (art. 20 da Convenção das Nações Unidas sobre o Direito do Mar).

inocente, apesar de estar envolvida no cometimento de um “delito”, não viola o Direito Internacional do Mar ou os termos da Convenção. Isso porque, prossegue o autor, a embarcação que opte por violar as condições da passagem inocente apenas “renuncia” a esse direito, que poderia lhe garantir uma passagem segura em águas territoriais estrangeiras, escolhendo realizar uma passagem “não inocente”. Nessas condições, argumenta o autor, o Estado que realiza a passagem “aceita a exposição legal de um trânsito que não é protegido pelo regime de passagem inocente, e ao fazê-lo aceita os riscos políticos e o perigo jurídico inerentes a tal operação”.⁴⁴⁴

Trata-se de um argumento equivocado. Pense-se, por analogia, na situação do diplomata que se encontra lotado no território de um Estado acreditado. Ele goza de certas imunidades mas se obriga a não se imiscuir em assuntos internos do Estado e a não violar as suas leis. Se ele adotar prática contrária – espionagem, por exemplo – isso significa que ele apenas está anuindo com a perda de suas garantias e com sua eventual “expulsão”? Não estaria ele violando os termos da Convenção de Viena sobre Relações Diplomáticas e assim o Direito Internacional? Parece que há claramente uma violação do Direito Internacional nos dois casos, na medida em que regras de Direito Internacional foram violadas, ainda que essa violação conduza a uma perda de determinado *status* tido como benéfico ao Estado violador.

A par das tradicionais modalidades de espionagem que são precedidas de intrusão territorial existem formas clandestinas de obtenção de segredos de Estado que ocorrem por via remota, através de redes de computadores ou de satélites de reconhecimento. A respeito da primeira modalidade, consolida-se o entendimento de que a espionagem internacional praticada no domínio cibernético, que envolva a obtenção remota de segredos através da intrusão em sistemas de outro Estado, não viola o Direito Internacional. Como observa Katharina Ziolkowski, ainda que o meio utilizado para obter acesso à informação visada possa consistir em uma violação ao

⁴⁴⁴ “In this case, while the submarine is involved in the commission of a delict, it may not be accurate to say it “violated” the international law of the sea, or the terms of UNCLOS. The Law of the Sea Convention states that foreign ships “shall comply” with coastal state regulations and laws, but this mandate is contingent on ships that are exercising the right of innocent passage. In this hypothetical, the submarine from State A merely relinquishes the right it otherwise might enjoy to travel in innocent passage and instead has chosen to transit in passage that is not innocent, and therefore unprivileged as a matter of law. While there is no right that may be claimed to travel in noninnocent passage, neither does there exist a law that has been violated in doing so. State A accepts the legal exposure of a transit that is unprotected by the regime of innocent passage, and in doing so accepts the political risk and legal jeopardy inherent in such operations”. KRASKA, James. Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters. *Columbia Journal of Transnational Law*, v. 54, 2015. p. 246.

Direito Internacional, o mero ato de copiar a informação por si só não consiste em uma violação.⁴⁴⁵ Remete-se, da mesma forma, à questão da “ilicitude colateral”. De qualquer modo, argumenta-se que a mera obtenção da informação através da espionagem cibernética não afronta o princípio da não-intervenção mesmo se a intrusão no sistema computacional exigir superar *firewalls* ou a “quebra” de senhas.⁴⁴⁶

Não obstante, é preciso apontar a existência de uma disposição da Convenção de Budapeste sobre Crimes Cibernéticos (2001) – ajustada no âmbito do Conselho da Europa mas assinada por outros países como Japão, Canadá, Austrália e Estados Unidos – que sinaliza o repúdio à métodos de acesso não autorizados a sistemas computacionais. Diz o art. 2 da Convenção, sob a epígrafe “Acesso ilegítimo”:

Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer como infração penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infração seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.⁴⁴⁷

Como se nota, o dispositivo determina que o acesso não autorizado de um sistema informático deve ser caracterizado como crime no Direito Interno dos Estados-partes, ainda que se exija para a configuração da conduta criminosa a violação de alguma medida de segurança ou uma intenção específica relacionada ao acesso. Todavia, não se firma na Convenção um compromisso dos Estados em não acessar sistemas computacionais uns dos outros – talvez seja mesmo por isso que os Estados Unidos sejam signatários da Convenção. Como consequência, não há uma norma internacional de proibição de acesso ilegítimo, mas apenas a obrigação de sua caracterização como crime segundo o Direito interno dos Estados. Isso reforça, inclusive, a postura irreflexiva dos Estados perante atos de

⁴⁴⁵ ZIOLKOWSKI, Katharina. Peacetime Cyber Espionage – New Tendencies in Public International Law. In: ZIOLKOWSKI, K. *op. cit.* p. 446.

⁴⁴⁶ NORTH ATLANTIC TREATY ORGANIZATION. **Tallin Manual**... *op. cit.* p. 47. A diferença entre o ataque cibernético e a espionagem cibernética reside justamente no fato de que aquele provoca dano aos sistemas computacionais e, portanto, a princípio implicaria algum grau de coerção a configurar uma violação ao princípio da não intervenção. *Ibidem.* p. 160.

⁴⁴⁷ O texto em português da Convenção pode ser acessado em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa428>

espionagem: os Estados punem como crime atos de espionagem interna e conduzem atos de espionagem externa mesmo sabendo que violam a lei doméstica do Estado alvo da operação.

Por fim, há a necessidade de definir a licitude de operações de espionagem conduzidas por satélites orbitais. Inicialmente verifica-se que o espaço cósmico é considerado patrimônio da humanidade, podendo ser livremente explorado para fins pacíficos (art. 1 do “Tratado sobre Princípios Reguladores das Atividades dos Estados na Exploração e Uso do Espaço Cósmico, inclusive a Lua e demais corpos celestes” ou “Tratado do Espaço Cósmico”), vedada qualquer tipo “de apropriação nacional por proclamação de soberania, por uso ou ocupação ou qualquer outro meio” (art. 2). A par disso, reconhece-se que a manutenção da paz e da segurança internacional são finalidades legítimas da exploração do espaço cósmico (art. 3).

Nessas condições, a colocação de satélites de reconhecimento em órbita e as atividades de vigilância por eles realizada foram consideradas, desde o início das viagens espaciais, uma forma de “utilização militar passiva do espaço cósmico” que não representam uma violação dos princípios que regem sua exploração e uso.⁴⁴⁸ Como explica Detlev Wolter, na negociação do Tratado do Espaço Cósmico as potências espaciais tiveram o cuidado de assegurar que nenhuma de suas disposições impedissem a realização das chamadas “atividades de suporte”, dentre elas a vigilância. Esse tipo de atividade era visto, especialmente pelos Estados Unidos, no contexto de sua estratégia de contenção nuclear (*nuclear deterrence*), como tendo um efeito estabilizante para a paz e segurança internacional através do mecanismo de “alertas” (*early warning*) e de exercício dos “meios técnicos nacionais de verificação” previstos no Tratado de Limitação de Armas Estratégicas (*Strategic Arms Limitation Treaty – SALT I*) e no Tratado de Mísseis Anti-Balísticos (*Anti-Ballistic Missile Treaty – ABM Treaty*), ambos de 1972.^{449 450} Mesmo a posição

⁴⁴⁸ Também sustentando a licitude da “vigilância orbital”, cf.: GREENBERG, Lawrence T.; GOODMAN, Seymour E.; SOO HOO, Kevin J. **Information Warfare and International Law**. National Defense University Press, 1998. p. 8.

⁴⁴⁹ WOLTER, Detlev. **Common Security in Outer Space and International Law**. United Nations Institute for Disarmament Research, 2005. p. 17-18; 27-28.

⁴⁵⁰ O SALT I, acordo bilateral ajustado entre Estados Unidos e União Soviética para limitação de armas ofensivas estratégicas, dispõem em seu art. V que: “1. *For the purpose of providing assurance of compliance with the provisions of this Interim Agreement, each Party shall use national technical means of verification at its disposal in a manner consistent with generally recognized principles of international law.* 2. *Each Party undertakes not to interfere with the national technical means of verification of the other Party operating in accordance with paragraph 1 of this Article.* 3. *Each Party undertakes not to use deliberate concealment measures which impede*

original da União Soviética de que o uso de satélites para a prática da espionagem seria algo ilícito, se rendeu ao argumento de que esses meios de verificação significavam o uso de satélites de reconhecimento, tanto no *SALT I* como no Tratado de Mísseis Anti-Balísticos.⁴⁵¹

É preciso observar, por derradeiro, que os “Princípios sobre o sensoriamento remoto da Terra a partir do Espaço Cósmico” (resolução da Assembleia Geral 41/65 de 3 de dezembro de 1986) estipula que as atividades de sensoriamento remoto devem ser conduzidas para “o benefício e interesse de todos os países” (princípio II). Além disso determina que o Estado que realiza a atividade deve, sob requerimento, entrar em consultas com o Estado cujo território é sensoriado, de forma a “disponibilizar oportunidades de participação” (princípio XII). Não obstante, parece que nem mesmo através dessas disposições pode-se dizer que a espionagem orbital seja proscrita, tendo em vista a possibilidade de resultar em algo benéfico para a comunidade internacional – por exemplo quando detecta um lançamento de um míssil balístico que poderia deflagrar uma guerra. Já a obrigação de iniciar um procedimento de consultas com o Estado sensoriado obviamente não se aplica às atividades clandestinas de sensoriamento tendo em vista ter por objetivo fomentar a cooperação entre os Estados, após requerimento do Estado sensoriado, o que implica seu conhecimento da atividade.

4.5.3 *O argumento da licitude da espionagem por exercício do direito à legítima defesa*

Uma das alternativas que vem sendo defendidas para a análise da licitude da espionagem internacional é associá-la ao direito à legítima defesa. Afirmam os partidários dessa análise que a espionagem internacional é permitida pelo Direito Internacional como corolário do direito à legítima defesa ao argumento de que “preparações defensivas apropriadas não podem ser feitas sem informação sobre potenciais ameaças”.⁴⁵²

verification by national technical means of compliance with the provisions of this Interim Agreement. This obligation shall not require changes in current construction, assembly, conversion, or overhaul practices”. A mesma disposição foi estabelecida no art. XII do *ABM Treaty*, também um acordo bilateral entre Estados Unidos e União Soviética.

⁴⁵¹ WOLTER, D. *op. cit.* p. 31.

⁴⁵² “*Appropriate defensive preparations cannot be made without information about potential threats*”. SCOTT, R. D. *op. cit.* p. 224.

De fato um princípio geral de Direito Internacional, o direito à legítima defesa está positivado em tratado, mais especificamente no art. 51 da Carta da ONU, sendo, inclusive, uma das poucas hipóteses em que a utilização da força é autorizada no Direito Internacional.⁴⁵³ É o conteúdo do dispositivo:

Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais.

Menciona-se no dispositivo a existência de um “direito inerente” à legítima defesa. O emprego da expressão nada mais significa, como observado pela CIJ no caso *Nicarágua v. Estados Unidos*, o reconhecimento da existência do direito à legítima defesa no costume internacional.⁴⁵⁴ Observou-se que o artigo 51 não regula todos os aspectos do exercício do direito à legítima defesa que são, por outro lado, bem estabelecidos no costume internacional, como a ideia de proporcionalidade e necessidade no emprego dos meios destinados à responder ao ataque armado.⁴⁵⁵ Desse modo, a verificação do direito à legítima defesa em duas fontes – um tratado (a Carta da ONU) e o costume internacional – foi considerada pela Corte como relação de coexistência de direitos, de conteúdos diversos, sendo que a superveniência do dispositivo convencional não revogou a regra costumeira.⁴⁵⁶

Nota-se ainda que o exercício do direito à legítima defesa está condicionado, por força da norma convencional, à ocorrência de um “ataque armado”. Logo, a legítima defesa é tratada no dispositivo no contexto da utilização da força como resposta a uma agressão, nada dizendo sobre questões relativas a preparações

⁴⁵³ A outra hipótese em que a utilização da força é permitida no Direito Internacional é sob autorização do Conselho de Segurança com base no capítulo VII da Carta da ONU.

⁴⁵⁴ INTERNATIONAL COURT OF JUSTICE. **Case Concerning Military...** *op. cit.* p. 94.

⁴⁵⁵ *Ibidem.* p. 94.

⁴⁵⁶ “It cannot therefore be held that Article 51 is a provision which “subsumes and supervenes” customary international law. It rather demonstrates that in the field in question, the importance of which for the present dispute need hardly be stressed. Customary international law continues to exist alongside treaty law. The areas governed by the two sources of law thus do not overlap exactly, and the rules do not have the same content”. *Ibidem.* p. 94.

defensivas. Seria, portanto, um artifício hermenêutico problemático extrair da literalidade do artigo um direito de se obter clandestinamente informações sigilosas de outro Estado como decorrência de um direito de se defender de eventuais ataques armados. Ou seja, numa lógica rasa, apegada à uma interpretação restrita do dispositivo, não faria sentido espionar para saber que serei atacado se somente posso me defender se efetivamente for atacado.

Todavia, uma interpretação do art. 51 em associação com o art. 2(4) da Carta, que traz a proibição genérica de uso da força, nos lembra que a prerrogativa da defesa da integridade territorial é condição necessária para o exercício independente do poder soberano do Estado. Para a manutenção de um sistema equilibrado de Estados delimitados, com base no respeito à integridade territorial e independência política – que é o que propõe a Carta da ONU – é necessário admitir que os Estados estabeleçam estruturas defensivas a fim de repelir eventuais ataques que, não sendo autorizados pelo Conselho de Segurança, serão fatalmente ilícitos perante o Direito Internacional. Portanto, sendo a legítima defesa um dos meios de garantia do direito à integridade territorial⁴⁵⁷, as preparações defensivas são necessárias para que possam viabilizar um efetivo exercício do direito à legítima defesa no caso de um eventual ataque armado. Pode-se formular então a seguinte premissa: se há o direito de se defender de um ataque, há o correspondente direito de se preparar para tanto. Logo, não há dúvidas de que os Estados possuem o direito de implementar aparatos defensivos nos limites do seu território, tais como radares de monitoração do espaço aéreo, fortes militares, escudos antimísseis, baterias antiaéreas etc.

Se considerarmos então que as preparações defensivas são necessárias para um adequado e eventual exercício do direito de legítima defesa diante de um ataque armado, deve-se aceitar por consequência que a utilização de medidas que permitem saber se um Estado será ou não alvo de um ataque é a ele autorizada. Assim, a premissa anteriormente proposta pode ser acrescida: se há o direito de se defender de um ataque, há o correspondente direito de saber se algum ataque ocorrerá, para que se possa preparar para tanto. De fato, havendo a possibilidade de ocorrência de ataques surpresas e de proporções catastróficas (ex: *Pearl Harbor*,

⁴⁵⁷ Como afirmou Bowett: “*The most obvious substantive right for which the right of self-defence serves as a means of protection is the right of territorial integrity, and it is in the defence of state territory that the right of self-defence is most clearly invoked*”. BOWETT, D. W. **Self-Defence in International Law**. Manchester University Press, 1958. p. 29.

as *blitz* da Alemanha nazista, *Hiroshima* e *Nagasaki*, invasão do *Kuwait*, ataques às torres gêmeas) – todos eles planejados sob sigilo e muitos ocorrendo mesmo em casos em que não há uma situação de beligerância previamente estabelecida entre as partes – há a correspondente necessidade de conhecer os riscos de efetiva ocorrência desses ataques. Estabelece-se, portanto, um forte argumento a favor do reconhecimento da licitude da espionagem internacional, **ao menos no que diz respeito aos segredos de Estado de natureza militar e política que se relacionem com uma posição hostil de outro Estado**. Como também defende Christopher Baker:

[...] para assegurar que o direito de legítima defesa mantenha seu significado substantivo, o Direito Internacional deve permitir aos Estados prever ataques armados. Logo, para que os estados se valham do direito positivo-codificado de legítima defesa, eles devem ter o direito de adquirir informação que irá indicar se eles enfrentam um iminente ataque armado.⁴⁵⁸

É importante observar porém, como alertou Julius Stone, que a espionagem que pode fazer acender a “luz vermelha”, indicando a preparação ou a iminência de um ataque armado, é a mesma que pode ativar a “luz verde”, demonstrando que o outro Estado está momentaneamente exposto a um ataque surpresa. Segundo o autor, o problema reside em saber “como cada lado irá ter certeza, em um sistema de espionagem reciprocamente tolerada, que a atividade do outro irá realizar apenas a salutar função da luz vermelha e não a perigosa função da luz verde”.⁴⁵⁹

De fato, não há garantias de que um Estado utilize a espionagem de informações classificadas apenas com propósitos defensivos. Mas isso não significa que o Direito Internacional não repudia prática contrária. Com efeito, como bem observa Craig Forcese, a espionagem conduzida como preparação para um ataque armado pode ser considerada uma ‘ameaça de uso da força’, proibida pela Carta da

⁴⁵⁸ “[...] in order to ensure that the right to self-defense retains substantive meaning, international law must permit states to predict armed attack. Therefore, for states to enjoy the positively-codified right to self-defense, they should retain the right to acquire information that would indicate whether they face imminent armed attack”. BAKER, C. D. *op. cit.* p. 1096.

⁴⁵⁹ “Spying may serve the common-interest function (which I might call “the red-light function”) of warning the spying state of the other’s preparations for surprise attack. Or it may serve the divisive and destructive function (which I may call the “green-light function”) for which it may still also be used in our time, namely, that of letting the spying side know that the other side is momentarily exposed to surprise attack [...] We still have to come to the question of how each side can be sure, in a system of reciprocally tolerated espionage, that the craft of the other are going to perform only the salutary red-light function, and not the dangerous green-light function”. STONE, J. *op. cit.* In: STANGER, R. J. *op. cit.* p. 42-43.

ONU e pelo Direito Internacional costumeiro nas circunstâncias em que a própria utilização da força seria considerada ilícita.⁴⁶⁰

Note-se ainda que entre a espionagem que antecipa um ataque armado e aquela que prepara um ataque, há uma terceira possibilidade, que é a espionagem que, mesmo fundamentada no exercício do direito à legítima defesa, não resulta na identificação de preparações hostis. Seria a “luz branca”, para seguir a figuração empregada por Julius Stone. Nesse sentido, a espionagem do Estado “A” que revela intenções amistosas do Estado “B”, contrariando expectativas de hostilidade anteriores, pode dissuadir inclusive a realização de um ataque preventivo⁴⁶¹ por parte daquele, contribuindo para um quadro de estabilidade e, em última análise, para a manutenção da paz internacional. Esse efeito será discutido no capítulo 6.

4.6 A escassez de parâmetros normativos como evidência da tolerância jurídica da espionagem internacional

Do estudo feito nas seções anteriores pôde-se verificar que a retórica da promoção da segurança permitiu a potencialização das capacidades dos serviços de inteligência, movimento que não foi acompanhado por maior limitação normativa da atividade. Pelo contrário, verificou-se que são escassas as normas de Direito Internacional aplicáveis ao exercício da espionagem estatal. As poucas regras a que se pode recorrer para encontrar alguma limitação à prática se aplicam de forma indireta, ou seja, não proscrevendo a espionagem por si só mas tutelando, por via reflexa, o sigilo da informação que se busca obter através da atividade.

Ocorre que, mesmo por essa forma indireta, é possível estabelecer *graus de proximidade* das normas aplicáveis a cada uma das três modalidades de espionagem analisadas, em relação inversa de proporcionalidade com o *nível de incerteza* que recai sobre cada uma delas. Quanto mais próxima estiver uma regra

⁴⁶⁰ “First, espionage conducted as preparation for an armed attack may be considered a “threat or use of force” precluded by the U.N. Charter and customary international law. It is, therefore, a violation of international law unless the use of force at issue is itself authorized by the Security Council under chapter VII of the U.N. Charter or is lawful as an exercise of self-defense”. FORCESE, Craig. Spies Without Borders: International Law and Intelligence Collection. **Journal of National Security Law and Policy**, 2011. p. 198-199.

⁴⁶¹ A questão da existência de um direito à “legítima defesa preventiva” ou “antecipatória” é extremamente controversa. Sobre a discussão pertinente, conferir: WAXMAN, Matthew C. Self-Defense and the Limits of WMD Intelligence. In: **Koret-Taube Task Force on National Security and Law**, Hoover Institution, Stanford University, 2010 e SHAW, M. N. *op. cit.* p. 1137-1140.

da hipótese fática a que destina sua aplicação, especialmente em termos hermenêuticos, menor serão as divergências teóricas a respeito. Assim, a aplicação das regras de proteção à privacidade individual para regular o exercício de atividades de coleta de informações privadas é inquestionável na doutrina e não encontra outros parâmetros “rivais” de regulação que poderiam ser igualmente aplicáveis em tese. Já em relação à espionagem econômica, como visto, há controvérsia sobre qual a regra cuja aplicação é a mais adequada para aferição de sua licitude – se a proteção do segredo de empresa no Direito de Propriedade Intelectual ou se na defesa da “soberania econômica”. Por último, há séria insegurança sobre quais regras de Direito Internacional a que se deve recorrer para definir a licitude da espionagem de segredos de Estado, isto é, se na noção de soberania e não-intervenção, se no direito de legítima defesa ou mesmo se na própria ausência de proibição expressa da atividade.

Essa relação curiosamente também demonstra o nível de *tolerância jurídica e política* dos Estados com as diferentes modalidades de espionagem, significando o grau em que a matéria é regulamentada pelo Direito e enfrentada politicamente, seja por pronunciamentos oficiais, negociações diplomáticas, fiscalização de órgãos da sociedade civil entre outras formas. A tolerância não se refere ao grau de permissividade jurídica da atividade de espionagem mas sim ao eventual silêncio que o Direito guarda em relação à determinada modalidade. Assim, por hipótese, um tipo de coleta de informações sigilosas que fosse detalhadamente regulado pelo Direito, ainda que isso resultasse em uma permissividade da sua prática em balizas amplas, representaria um grau de tolerância jurídica baixo. Da mesma forma, não se aborda aqui o grau de *tolerância prática* da atividade, que diz respeito à resposta material que o Estado alvo da espionagem dá à operação, isto é, se ele responde com o aumento de sua segurança e melhoria de técnicas de contrainteligência, ou mesmo algum tipo de represália – ações que em regra não guardam relação de proporcionalidade com o grau de proximidade da norma e o nível de controvérsia.

Sendo assim, a espionagem de informações privadas de particulares é aquela a que corresponde o menor grau de tolerância jurídico-política, principalmente porque é considerada uma violação a direitos humanos e porque sofre um forte controle em duas dimensões: *internamente*, pela legislação doméstica, por vezes até mesmo por disposições constitucionais de proteção à privacidade, e pelos mecanismos oficiais de fiscalização do serviço de inteligência, além da opinião

pública; e *externamente*, através do sistema de proteção internacional dos direitos humanos, sob fiscalização de diversos órgãos internacionais. Sua prática às margens dos limites legais é normalmente respondida com processos judiciais em foros internacionais, cujas sentenças são vinculantes aos Estados, sendo um exemplo da força da tutela internacional dos Direitos Humanos.

Por sua vez, a espionagem de segredos de empresa revela um grau de tolerância médio. De um lado tem o potencial de somar prejuízos bilionários e os Estados sinalizam com um nível de repúdio maior à prática em comparação com períodos anteriores, o que se verifica nos recentes atritos entre Estados Unidos e China. De outro lado, os Estados até o momento nunca apresentaram a questão a um órgão internacional, limitando-se, na maioria das vezes, a protestos a nível diplomático e político. Mesmo a acusação que os Estados Unidos fizeram aos oficiais militares chineses em cortes domésticas teve mais pretensões políticas do que efetivamente judiciais (cf. Introdução). Além disso, por ser praticada precipuamente no domínio cibernético, a espionagem econômica implica *dificuldades de atribuição*, sendo complexo aferir qual a origem da atividade de coleta.⁴⁶²

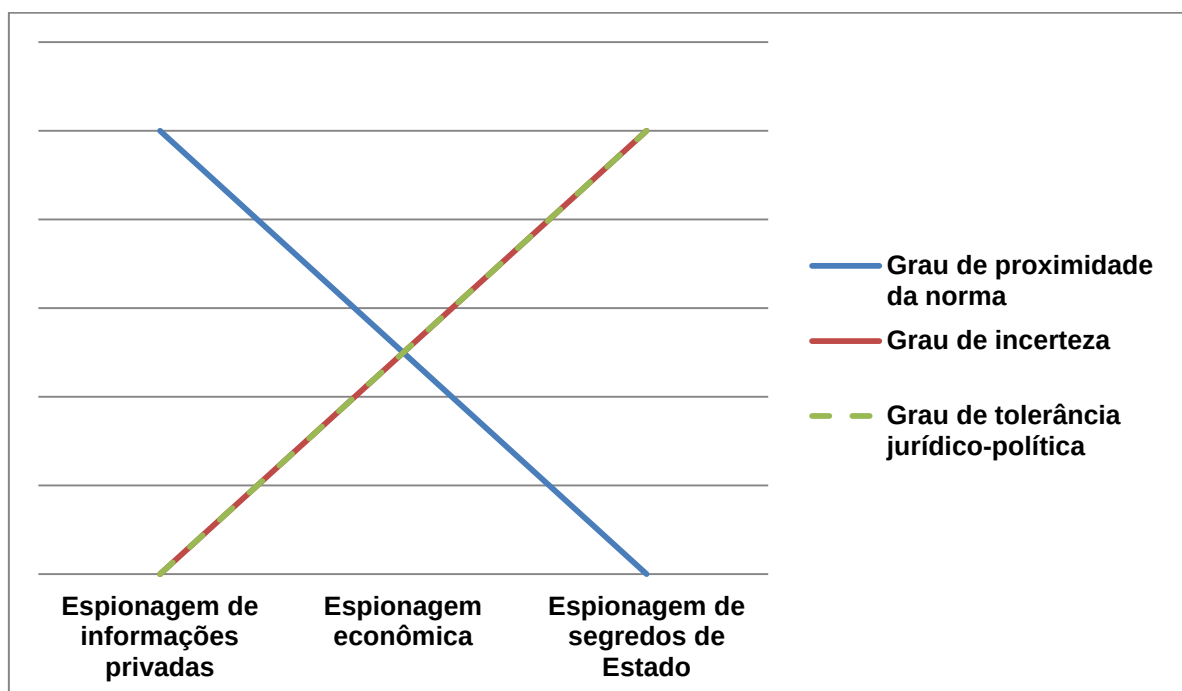
Já a espionagem de segredos de Estado de natureza política e militar demonstra um alto grau de tolerância da comunidade internacional pois raramente é levada a protesto a nível oficial. Mesmo porque, o protesto contra um ato de espionagem de informações classificadas normalmente implicaria a revelação de vulnerabilidades na segurança do Estado, do segredo ou de parcela dele, bem como na sinalização para o Estado coletor acerca do valor da informação – a não ser que se trate de uma engenhosa operação de engano (*deception*). Mais que isso, o prejuízo gerado pela espionagem de segredos de Estado a princípio não é quantificável como ocorre com a espionagem econômica; ele é estratégico, e muitas vezes apenas se revela a longo prazo, do que é um bom exemplo a obtenção do segredo de fabricação da bomba atômica pela União Soviética, como descrito na seção 3.3. Daí sua maior tolerância em termos políticos e jurídicos.

⁴⁶² WILLIAMS, Robert D. (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action. *The George Washington Law Review*, v. 79, 2011. p. 1183.

É possível, portanto, traçar a seguinte relação entre essas variáveis:

Modalidade de espionagem	Grau de proximidade da norma	Grau de incerteza	Grau de tolerância jurídico-política
Informações privadas	Alto	Baixo	Baixo
Econômica	Médio	Médio	Médio
Segredos de Estado	Baixo	Alto	Alto

Graficamente essa relação pode ser representada da seguinte forma:



O próprio “efeito irreflexivo” discutido na Introdução, que é a forma díspare com que os Estados abordam atos de espionagem de um outro Estado em relação aos atos análogos que conduz, só é possível graças à notória fragmentariedade e imprecisão das regras de Direito Internacional aplicáveis, insuficientes para disciplinar a atividade de forma compreensiva. Diante de poucas regras de Direito Internacional que limitem a coleta de informações externamente, especialmente de segredos de Estado de natureza política e militar, os Estados se veem encorajados a potencializar a prática da espionagem internacional e ao mesmo tempo livres para definir, a nível doméstico, suas próprias regras de repressão de atos de espionagem que lhes são desfavoráveis.

De qualquer forma, os diferentes níveis de tolerância das três modalidades de espionagem analisadas anteriormente sugerem uma maior propensão da comunidade internacional a regular a espionagem de informações privadas e de

segredos de empresa. Certamente nesses dois domínios há maiores chances de se alcançar níveis superiores de limitação ao que hoje se tem, se comparados à espionagem de segredos de Estado que, como visto, possui alto grau de tolerância.

5 UMA LEITURA REALISTA DAS CAUSAS DA TOLERÂNCIA DA ESPIONAGEM INTERNACIONAL

"In essence, Political Realism is as old as political thought. It arises inevitably whenever people become fully aware of the failure of repeated attempts to 'reform' political life, to create a 'better world' [...] History, which is the burial ground of such attempted changes, is also the birthplace of realist disillusionment. And disillusionment, in turn, gives rise to realism".⁴⁶³ (John H. Herz)

Estabelecidas tais verificações sobre a graduação da tolerância das diferentes modalidades de espionagem, cabe agora aprofundar o estudo sobre as razões que fazem perpetuar a ausência de regulamentação da atividade no Direito Internacional. Qual a razão do silêncio e quais são as possibilidades reais de que atividades de espionagem venham a ser reguladas pelo Direito Internacional? Esse tipo de análise envolve considerações metajurídicas; é algo que extrapola o estudo da Ciência do Direito para atingir a investigação sobre as formas de comportamento e condições de cooperação entre os Estados – objeto da Teoria das Relações Internacionais.

Regular relações entre Estados e outros sujeitos de Direito Internacional sempre se mostrou uma tarefa mais dificultosa se comparada ao processo de criação de normas no âmbito doméstico. Na ausência de um órgão legislativo central, a manifestação normativa do Direito Internacional normalmente depende da acomodação de interesses plurais, muitas vezes conflitantes, dos próprios destinatários da norma, em demoradas negociações até o ajuste de um tratado internacional, ou pela paulatina adoção de um padrão de comportamento ou de valores principiológicos pelos Estados.

Nesse cenário, é verdade, algumas facetas das relações entre os Estados apresentam maior aptidão à regulação do que outras. Situações em que há uma forte convergência de interesses entre os vários Estados envolvidos normalmente conduzirão a um ambiente de *cooperação* ao invés de *confrontação* – não simplesmente uma cooperação puramente pragmática mas sim, e principalmente, algo disciplinado pelo Direito Internacional. As regras que disciplinam a navegação marítima e a aviação civil internacional são dois bons exemplos: os interesses

⁴⁶³ HERZ, John H. **Political Realism and Political Idealism**: a study in theories and realities. The University of Chicago Press, 2 ed., 1959. p. 27.

recíprocos que possuem os Estados em realizar tais atividades – na verdade a própria viabilidade de sua realização – os motivam a cooperar e regulamentar seu exercício. Isso pode ocorrer mesmo sem o ajuste de um tratado formal, através da prática costumeira, como ocorreu na fase embrionária do Direito do Mar, por exemplo.

De fato, na convergência de interesses se pode notar facilmente um importante elemento que motiva a cooperação, mas existem outros fatores que interferem no processo de decisão das autoridades estatais em ajustar ou não um compromisso internacional. A questão é de extrema complexidade, o que se prova pelo fato de que ainda não se formulou uma teoria que seja capaz de apresentar uma análise compreensiva de quais são exatamente esses fatores de motivação e quais as precisas condições em que os Estados recorrem ao Direito Internacional para regulamentar aspectos de suas relações e atividades.⁴⁶⁴ Não obstante, da Teoria das Relações Internacionais, se pode extrair modelos que buscam descrever as condições de cooperação entre os Estados em linhas genéricas.

Dessas muitas teorias, sugere-se investigar – pelos critérios definidos na Metodologia – as causas da tolerância da espionagem internacional sob o modelo do *realismo político*.

5.1 Revisitando o realismo político através dos estereótipos da crítica

Toda teoria é uma tentativa de simplificação da realidade. Criam-se teorias para que fenômenos complexos – naturais, físicos, sociais etc. – possam ser traduzidos em linguagem e modelos lógicos, e assim então possam ser inteligíveis. No domínio das Relações Internacionais, da mesma forma, as teorias buscam explicar os padrões de comportamento entre os Estados e outros atores e os resultados de suas interações sociais.

Como já antecipado na Metodologia, as várias teorias das Relações Internacionais são agrupadas por razões de sistematização; não se tratam de “tradições teóricas monolíticas e homogêneas”.⁴⁶⁵ Não obstante, os elementos comuns entre umas e outras, aquilo sobre o que seus autores concordam, ao menos

⁴⁶⁴ Segundo Ashley Deeks, “One reason for a lack of theories predicting specific factors that motivate states to turn to international law at time X or Y may be the fact that these decisions are contingent on so many factors”. DEEKS, A. An International Legal... *op. cit.* p. 320, nota de rodapé 102.

⁴⁶⁵ BURCHILL, S. *et. al. op. cit.* p. 18.

em linhas genéricas, permitem seu agrupamento em “escolas”. Isso vale para o realismo político – talvez mais do que para qualquer outra linha de pensamento das Relações Internacionais – que se desdobra nas vertentes clássica (Edward Carr; Hans Morgenthau; John Herz entre outros) e estrutural (ou neorealismo) e suas divergências internas entre o realismo defensivo (John Herz; Kenneth Waltz) e ofensivo (John Mearsheimer). É preciso concentrar naquilo em que essas variantes se assemelham, isto é, naquelas proposições que permitem que sejam elas reunidas sob a “etiqueta” realista e, principalmente, o que as distingue das proposições de teorias rivais.

Nesse sentido, o realismo político, analisado de forma abrangente, trabalha com as seguintes premissas⁴⁶⁶:

- a) *Atores unitários*: Inicialmente, considera os Estados os principais atores na política mundial, especialmente aqueles que detêm maior poder. Obviamente, não ignora a existência e até mesmo eventual influência de atores não-estatais; apenas direciona seu foco à figura do Estado;
- b) *Sociedade internacional anárquica*: Esses Estados se relacionam em um ambiente desprovido de hierarquia supraestatal, isto é, uma sociedade anárquica;
- c) *Racionalismo, segurança e poder*: Essa lógica de atuação é orientada racionalmente sobre considerações de poder em função da segurança, e o resultado disso é a permanente competição entre os Estados. Logo, a política internacional envolve a mitigação e administração dos conflitos, não sua eliminação – um objetivo utópico;
- d) *Relativização*: Por fim, essa competição se resume a um “jogo de soma zero”, em que os ganhos e perdas de poder por parte dos Estados são avaliados de forma relativa. Se algum Estado ganha poder, outro necessariamente perde. Por essa razão a cooperação entre os Estados ocorre periféricamente pois acaba se convertendo em competição a longo

⁴⁶⁶ O que se segue é um compilado adaptado de MEARSHEIMER, John J. **The Tragedy of Great Power Politics**. W. W. Norton & Company, 2001. p. 29-30 e 38-40 e DONNELLY, J. *op. cit.* In: BURCHILL, S. *et. al. op. cit.* p. 30-32.

prazo. A raiz das relações entre os Estados é necessariamente conflituosa.

A partir daí se constroem teorias variantes sobre proposições que ora relaxam, ora extremam, em grande medida, as premissas realistas nucleares. Jeffrey Legro e Andrew Moravcsik identificaram esse problema ao notar que muitas teorias que se pretendem realistas destoam tão sensivelmente das proposições originais – que efetivamente identificam o realismo como corrente teórica – que não podem ser consideradas uma variante legítima, por vezes até se confundindo com teorias rivais.⁴⁶⁷ Essa miríade de “teorias realistas” gera confusão e por vezes favorece interpretações equivocadas sobre o que, de fato, são proposições realistas.

E assim o *realismo político* hoje é por muitos visto como uma teoria das Relações Internacionais já ultrapassada, que teve seu valor, reconhecem, num paradigma político de confrontação bibolar característico da guerra fria, mas que hoje não mais representaria uma descrição adequada do novo modelo de organização multipolar e globalizado.⁴⁶⁸ Novas teorias atacam o caráter *pessimista* de suas proposições e denunciam seu excessivo enfoque nas relações de poder e segurança entre os Estados.

Os *liberalistas*, por exemplo, demonstram um maior otimismo com a expansão da democracia liberal pelo globo e, como consequência, com as condições de manutenção da paz internacional.⁴⁶⁹ Do ponto de vista metodológico, invertem a ótica estrutural neorrealista – ou seja, sua análise focada em fatores supranacionais – para investigar os elementos domésticos que interferem na política externa dos Estados.⁴⁷⁰

⁴⁶⁷ LEGRO, Jeffrey; MORAVCSIK, Andrew. Is anybody still a realist? **International Security**, v. 24, n. 2, 1999.

⁴⁶⁸ Como reconhece o realista Kenneth Waltz: “Some students of international politics believe that realism is obsolete”. WALTZ, Kenneth. Structural Realism after the Cold War. **International Security**, v. 25, n. 1, 2000. p. 5.

⁴⁶⁹ De fato, o entusiasmo com o fim da Guerra Fria levou alguns autores a prognosticar o início de um novo período de paz nas relações internacionais, ao mesmo tempo em que denunciavam o pessimismo que dominara a maior parte do século XX. Entre eles FUKUYAMA, Francis. **The End of History and the Last Man**, The Free Press, 1992 – especialmente no capítulo “Our Pessimism” e LEBOW, Richard Ned. The long peace, the end of the cold war, and the failure of realism. **International Organization**, v. 48, n. 2, 1994.

⁴⁷⁰ Por exemplo: SLAUGHTER, Anne-Marie. **A New World Order**. Princeton University Press, 2004 e SLAUGHTER, Anne-Marie. International Law in a World of Liberal States. **European Journal of International Law**, v. 6, 1995.

Também como alternativa ao realismo político, os *institucionalistas* enfatizam as relações de cooperação entre os Estados e as dimensões de interdependência da sociedade internacional. A adesão de Estados a *instituições* comuns – entendidas não apenas como organizações internacionais formais, como a ONU, por exemplo, mas todo *regime* de normas e procedimentos que regulamentam o comportamento dos Estados e controlam seus efeitos – facilitariam a cooperação futura ao reduzir os custos de transação.⁴⁷¹

Já as teorias *construtivistas* focam no caráter social das relações humanas. O indivíduo é concebido como um ente cuja identidade é construída socialmente; são as relações sociais que “constroem” a pessoa e permitem ser o que ela é. Os Estados, como entes sociais, também se inserem na mesma lógica: suas relações moldam sua identidade e o resultado disso é uma construção social. Nesse contexto, as preferências dos Estados não são fixas – como na proposição realista de que os Estados almejam poder – mas sim, variáveis construídas pelas estruturas sociais.⁴⁷²

Paralelamente há uma multitude de outras teorias de cunho crítico com alvo na condição de desigualdade entre os Estados. Incluem, mas não se limitam a, teorias de inspiração *marxista* que denunciam as formas de dominação capitalista das “grandes potências” e a posição marginal de países do chamado “terceiro mundo”. Somam-se a isso teorias *feministas* que atacam a apropriação masculina da política internacional, da cultura da guerra e mesmo do estudo das Relações Internacionais. Enfim, são várias as alternativas teóricas ao realismo político.⁴⁷³

Fora dos departamentos de Relações Internacionais das universidades, o realismo político ainda sofre ataques dos jusinternacionalistas, irredimidos com aquilo que acreditam ser assertivas realistas de que as regras de Direito Internacional e a moral exercem pouca ou nenhuma influência no comportamento dos Estados. Como afirma Thomas Franck, “Obediência às regras, na mente dessas pessoas [realistas], é um sinal de fraqueza. É uma indigna abdicação das

⁴⁷¹ KEOHANE, Robert O.; NYE, Joseph S. **Power and Interdependence**, Little, Brown, 1977.

⁴⁷² WENDT, Alexander. Collective identity formation and the international state. **American Political Science Review**, v. 88, 1994; ONUF, Nicholas. **World of Our Making: Rules and Rule in Social Theory and International Relations**, University of South Carolina Press, 1989.

⁴⁷³ Para uma apresentação sintética dessas muitas teorias conferir: GRIFFITHS, Martin. **Fifty Key Thinkers in International Relations**. Routledge, 1999 e BURCHILL, S. *et. al. op. cit.*

prerrogativas e responsabilidades do poder nacional”.⁴⁷⁴ Ou como diz Allen Buchanan:

Os realistas negam que exista uma obrigação moral não instrumental de promover o estado de direito internacional [*rule of international law*] porque eles acreditam que, dada a natureza das relações internacionais como eles a concebem, o direito internacional nunca será capaz de fazer qualquer contribuição à justiça. (Além disso, eles podem inclusive sustentar que o conceito de justiça não tem nenhuma aplicação nos assuntos internacionais). Dada a fraqueza do Realismo, que tem sido crescentemente exposta nos últimos anos, esse argumento de negar que exista qualquer obrigação moral não instrumental para apoiar o projeto do direito internacional é pouco conclusivo.⁴⁷⁵

Desse modo, essa leitura é (irrefletidamente) propagada na literatura do Direito Internacional, em que muitas vezes o realismo é responsabilizado pelo que há de mau no mundo. Antônio Augusto Cançado Trindade, por exemplo, ao comentar a questão da limitação da posse e utilização de armas nucleares, afirma que a ideia da dissuasão nuclear (*nuclear deterrence*) é uma artificialidade da postura dos realistas políticos, “em sua característica subserviência ao poder político” e não ao Direito, a eles atribuindo também a culpa das ambiguidades que permeiam a proibição “formal e expressa pelo Direito Convencional Internacional” da ameaça de utilização de armas nucleares.⁴⁷⁶ O autor vai além: ao comentar a importância das conferências da ONU para a cooperação internacional

⁴⁷⁴ “Obedience to rules, in the minds of these persons, is a sign of weakness. It is an unworthy abdication of the prerogatives and responsibilities of national power”. FRANCK, Thomas M. **The Power of Legitimacy among Nations**. Oxford University Press, 1990. p. 4.

⁴⁷⁵ “Realists deny that there is a non-instrumental moral obligation to promote the rule of international law because they believe that, given the nature of international relations as they understand it, international law will never be capable of making a significant contribution to justice. (In addition, they may in fact hold that the concept of justice has no application to international affairs.) Given the weaknesses of Realism, which have been increasingly exposed in recent years, this reason for denying that there is a non-instrumental moral obligation to support the project of international law is hardly conclusive”. BUCHANAN, Allen. *The Legitimacy of International Law*. In: BESSON, Samantha; TASIOLAS, John. **The Philosophy of International Law**, Oxford University Press, 2010. p. 89. Outros autores denunciam aquilo que denominam de “influência corrosiva” do realismo no Direito Internacional, por, segundo assim o interpretam, sustentar a tese de que “a moralidade política não alcança além das fronteiras do Estado”. Cf. BESSON, S. et. al. *op. cit.* p. 3.

⁴⁷⁶ “The adoption of the 1967 Tlatelolco Treaty, the 1985 Rarotonga Treaty, the 1995 Bangkok Treaty and the 1996 Pelindaba Treaty disclosed the shortcomings and artificiality of the posture of the so-called political “realists” which insisted on the suicidal policy of nuclear deterrence, in their characteristic subservience to power politics”. TRINDADE, A. A. C. *op. cit.* parte V, p. 36. Mais adiante no texto a crítica se repete: “Yet, despite the clarity of the formidable threat that nuclear weapons represent, their formal and express prohibition by conventional International Law has most regrettably remained permeated by ambiguities, due to resistances on the part of the so-called “realists” of Realpolitik, always at the service of power rather than Law”. *Ibidem*. p. 41.

responsabiliza os realistas quem, “em sua característica miopía, tentaram, sem surpresa e em vão, minimizar o diálogo universal” que delas resultou.^{477 478}

Especificamente em relação ao estudo da espionagem internacional, autores alegam – igualmente viciados pela crítica superficial – que o realismo político é um paradigma inadequado de análise. Christopher Baker afirma que o realismo falha em explicar a tolerância da espionagem internacional e não é capaz de assimilar “os benefícios cooperativos que advêm para todos os Estados como resultado da espionagem”.⁴⁷⁹ Raphael Bitton, ao sugerir a necessidade de se observar regras morais para o exercício da espionagem, considera que a adoção das premissas realistas impediria tal objetivo, pois entende que “para os realistas, aderir a obrigações morais à expensa de interesses nacionais [...] não faria sentido”.⁴⁸⁰

Se o que dizem todos esses autores a respeito do realismo for verdade, então a construção dessa tese padece de uma contradição insuperável: propõe a análise de uma atividade estatal (a espionagem internacional) sob uma ótica jurídica, argumentando a existência de regras que limitam seu exercício e, ao mesmo tempo, sob o prisma político, mas sustentada em um paradigma que aparentemente descredencia o valor das mesmas regras de Direito Internacional que diz ter alguma eficácia regulamentar. Todavia, é preciso cautela antes de apontar qualquer traço de repúdio ao Direito Internacional e à moralidade nas teorias realistas, que desacredite qualquer possibilidade de diálogo entre eles.

⁴⁷⁷ “It is today generally acknowledged that such transparent “State-societal interaction” has stressed the relevance of universal principles and social values, has fostered multilateralism and established a pattern of change in ideas aiming at the general improvement of the human condition. These points have simply been missed by the so-called “realists”, who, in their characteristic myopia, have, not surprisingly, attempted, in vain, to minimize the universal dialogue emerging of the recent UN World Conferences”. *Ibidem.* parte VIII, p. 266.

⁴⁷⁸ Tudo isso é ainda agravado por uma carga de preconceito associada à impopular tônica intervencionista da política externa norte-americana durante a guerra fria, fortemente influenciada pelo projeto realista de Henry Kissinger, quem foi Conselheiro de Segurança Nacional do Presidente Richard Nixon no final dos anos 60 e Secretário de Estado de 1973 a 1977 na gestão de Gerald Ford.

⁴⁷⁹ “Examined in light of the realist approach to international relations, states spy on one another according to their relative power positions in order to achieve self-interested goals. This theoretical approach, however, not only fails to explain international tolerance for espionage, but also inadequately captures the cooperative benefits that accrue to all international states as a result of espionage”. BAKER, C. D. *op. cit.* p. 1091-1092.

⁴⁸⁰ “realists do not argue that espionage is morally justified but rather that states do not need to morally justify it in the first place. To realists, adhering to moral duties at the expense of national interests (represented, in this case, by the need to spy) would not make sense. A state that eschews espionage to comply with a moral duty puts its interests at risk, and this, given the nature of the international sphere, could be fatal”. BITTON, Raphael. The Legitimacy of Spying Among Nations. *American University International Law Review*, v. 29, n. 5, 2014. p. 1014-1015.

De fato, a crítica incisiva que é feita hoje ao realismo político é convenientemente focada em versões mais radicais da teoria, ignorando proposições moderadas do chamado *realismo clássico*, sensível a questões normativas nas relações internacionais. Como bem observado por William Scheuerman:

[...] críticos do Realismo tornaram as coisas muito fáceis para eles mesmos ao adotar uma simplista e por vezes caricaturizada interpretação do Realismo. Eles regularmente ignoram versões de teoria internacional Realista – e especialmente fortes variantes normativas do Realismo de metade de século [XX] [...] que se sustentam em ideias mais sofisticadas e politicamente atraentes do que aquelas que lhes são atribuídas praticamente universalmente. Apesar de que continuar a reciclar o senso comum certamente nos ofereceria um caminho mais fácil, qualquer um comprometido com a integridade intelectual tem uma responsabilidade de fazer melhor que isso.⁴⁸¹

Para ir além dos estereótipos repetidos pela crítica superficial é necessário revisitar as bases de determinada teoria a fim de revelar sua essência, e assim realizar uma leitura mais fiel do que aquela que é fruto da propagação de equívocos e simplificações. Felizmente, mesmo defensores de teorias alternativas notaram o valor descritivo do modelo realista e alertaram para leituras apressadas que dele se possa extrair. Anne-Marie Slaughter, um dos maiores expoentes do liberalismo nas Relações Internacionais, ainda que repetindo velhos *clichés* sobre o Realismo em outros trabalhos⁴⁸², reconhece:

Jusinternacionalistas que avaliam a teoria Realista devem ter cuidado para compreender a lógica interna do paradigma Realista, ao menos para dispersar qualquer noção de que os Realistas são de alguma forma imorais ou amam o poder para seu próprio bem. [...] Além do mais, apesar de o Realismo ser provavelmente mais conhecido entre os jusinternacionalistas por rejeitar qualquer efeito causal das normas de Direito Internacional no sistema internacional,

⁴⁸¹ “Cosmopolitans and many other critics of Realism have made things too easy for themselves by embracing a simplistic and occasionally caricatured interpretation of Realism. They regularly ignore versions of Realist international theory – and especially sound normatively minded variants of mid-century Realism, described in the present volume as *Progressive Realism* – which rest on more sophisticated and politically appealing ideas than those pretty much universally ascribed to it. Although continuing to recycle conventional wisdom would certainly offer us all an easier path, anyone committed to intellectual integrity has a responsibility to do better”. SCHEUERMAN, William E. **The Realist Case for Global Reform**, Polity Press, 2011. p. 4.

⁴⁸² Como o faz por exemplo em SLAUGHTER, A. *International Law in a World... op. cit.* p. 507.

boa parte da estrutura e substância do Direito Internacional tradicional parece ter sido construída sobre fundações Realistas.⁴⁸³

Como também foi observado por W. Julian Korab-Karpowicz, ao comentar sobre a distinção entre o realismo clássico e o radical, ressalta que aquele não se trata da doutrina maquiavélica de que tudo é justificado pela razão do Estado, da mesma forma que não envolve glorificação do conflito e não rejeita a possibilidade de julgamento moral na política internacional.⁴⁸⁴

Sendo assim, uma crescente frustração com a forma com que autores clássicos são lidos sem o devido cuidado⁴⁸⁵ caracteriza um recente movimento revisionista que propõe o retorno aos autores realistas de meados do século XX.⁴⁸⁶ Especificamente no que diz respeito a Hans J. Morgenthau, um dos mais influentes deles (cf. seção 5.1.2), tem havido um

notável reempenho com a substância de seu pensamento, um empenho frequentemente aliado à alegação de que seu realismo não é apenas mais complexo do que nós fomos levados a crer, mas de considerável maior relevância contemporânea do que nós havíamos imaginado.⁴⁸⁷

⁴⁸³ “International lawyers assessing Realist theory must be careful to understand the internal logic of the Realist paradigm, if only to dispel any notion that Realists are somehow immoral or love power for its own sake. On the contrary, as the name suggests, Realists perceive that they are describing the realities of the international system, however unpleasant they may be. [...] Further, although Realism is probably best known among international lawyers for rejecting any causal role for international legal norms in the international system, much of both the structure and substance of traditional international law appears to be built on a Realist foundation”. SLAUGHTER, Anne-Marie. *International Law and International Relations. Collected Courses of the Hague Academy of International Law*, 2000. p. 33.

⁴⁸⁴ KORAB-KARPOWICZ, W. Julian. Political Realism in International Relations, *The Stanford Encyclopedia of Philosophy*, 2013. Disponível em: <http://plato.stanford.edu/archives/sum2013/entries/realism-intl-relations/>

⁴⁸⁵ Como aponta Oliver Jüterssonke, há uma “[...] acute frustration with the way ‘classical’ authors continue to be appropriated for a particular ‘tradition’, with little appreciation for the gaping chasm between standard renditions and a more nuanced, contextual reading of works that are considered as part of the canon”. JÜTERSONKE, Oliver. The image of law in Politics among Nations. In: WILLIAMS, Michael C. *Realism Reconsidered: The Legacy of Hans Morgenthau in International Relations*, Oxford University Press, 2007. p. 93.

⁴⁸⁶ Por exemplo: SCHEUERMAN, W. . *op. cit.*; WILLIAMS, M. C. *op. cit.* e NEACSU, Mihaela. **Hans J. Morgenthau’s Theory of International Relations: Disenchantment and Re-Enchantment**. Palgrave Macmillan, 2009. Conferir também a proposta de Yan Xuetong de um “realismo moral” com inspiração no realismo clássico em: XUETONG, Yan. Political Leadership and Power Redistribution. *The Chinese Journal of International Politics*, v. 9, n. 1, 2016.

⁴⁸⁷ “there has been a notable re-engagement with the substance of Morgenthau’s thinking, an engagement often allied to the claim that his realism is not only more complex than we have often been led to believe, but of considerably greater contemporary relevance than we have imagined”. WILLIAMS, M. C. *op. cit.* p. 1-2.

Seguindo essa proposta, sugere-se aqui identificar os principais argumentos e proposições das teorias realistas clássicas com o objetivo de estabelecer um quadro mais fiel sobre o realismo político e verificar se as críticas que lhe são dirigidas são ou não justificáveis.

Apesar de encontrar correspondência em filosofias políticas anteriores, como a ideia de estado de natureza de Thomas Hobbes e o enfoque no poder no pensamento de Maquiavel⁴⁸⁸ (o que poderíamos reunir sob a categoria “realismo primitivo”), o surgimento do realismo político como uma corrente de proposições mais consistentes pode ser identificado nos meados do século XX. Autores perplexos com a desintegração da Liga das Nações e a ineficácia do Pacto Kellog-Briand de 1928 começaram a questionar as crenças idealistas que inspiraram o período entre guerras. Sua agenda se concentra a partir de então em buscar respostas para perguntas tais como: quais são as principais fontes de estabilidade e instabilidade a nível internacional? Como funciona o “balanceamento de poder” entre os Estados, quais os fatores que influenciam seu equilíbrio e qual é a sua configuração ideal? Como as grandes potências devem se comportar umas em relação às outras e em relação aos Estados mais fracos?⁴⁸⁹

Três autores se destacam na fase inicial do realismo: o inglês Edward Hallett Carr (1892–1982) e os alemães Hans Morgenthau (1904-1980) e John Herz (1908-2005).⁴⁹⁰ Nas seções seguintes serão apresentados os principais argumentos e proposições de cada um desses autores para ao final resumir as teses centrais do realismo político clássico.

Antes disso, vale ser antecipada a constatação de que havia interessantes similaridades entre esses autores que extrapolavam a mera afinidade teórica. Como observou William Scheurman, tanto Morgenthau quanto Herz tinham formação jurídica e no início de suas carreiras estavam ligados a Hans Kelsen – apesar de Carr nunca ter recebido treinamento jurídico.⁴⁹¹ Morgenthau teve ainda íntima relação intelectual com Carl Schmitt e suas teses exerceram entre si forte

⁴⁸⁸ DONNELLY, J. *Realism. op. cit.* p. 30.

⁴⁸⁹ GRIFFITHS, M. *op. cit.* p. 2.

⁴⁹⁰ William Scheurman, em sua releitura do realismo, sugere a reunião desses autores na categoria que denomina de “realismo progressivo”, em que inclui ainda Reinhold Niebuhr (1892 – 1971) – quem influenciou o pensamento de Carr e Morgenthau – Frederick Schuman (1904 – 1981), Georg Schwarzenberger (1908 – 1991) e Arnold Wolfers (1892 – 1968). Cf. SCHEUERMAN, W. *op. cit.* p. 5-6.

⁴⁹¹ *Ibidem.* p. 8-9.

influência⁴⁹², o mesmo se podendo dizer em relação a Hersch Lauterpacht.⁴⁹³ Outra semelhança merece nota: se atualmente o realismo é visto como uma manifestação do conservadorismo político da direita – outra caricaturização superficial dentre as muitas que se pretende aqui afastar – em meados do século XX poderia ser associado politicamente com a esquerda. Naturalmente, como judeus alemães num período de ascensão nazista, Morgenthau e Herz se aproximaram de ideias e políticas socialistas⁴⁹⁴ e mesmo Carr, na Inglaterra, se inclinou radicalmente para o socialismo.⁴⁹⁵ Além disso, a tônica marxista é perceptível em suas obras, como pode ser observado a seguir.

5.1.1 Edward Hallet Carr

Na obra *The Twenty Years' Crisis* – originalmente publicada em 1939, com uma segunda edição em 1946 – Carr ataca o discurso utópico que, segundo ele, dominou o pensamento político no período entre-guerras, ao que opõe então sua visão “realista”. A pretensa universalidade da moral invocada no projeto idealista é denunciada por Carr sob aquilo que denomina de *harmonia de interesses*. Trata-se da tendência que grupos dominantes têm de refletir seus valores e preferências para toda a comunidade, de forma a “justificar e manter sua posição”, propagando a ideia

⁴⁹² O chamado “diálogo oculto” (“*hidden dialogue*”) entre Morgenthau e Schmitt Martti é discutido detalhadamente em KOSKENNIEMI, M. **The Gentle...** *op. cit.* Capítulo 6. Dois outros estudos no mesmo sentido podem ser lidos em: BROWN, Cris. *The Twilight of International Morality?* Hans J. Morgenthau and Carl Schmitt on the end of the *Jus Publicum Europaeum*. In: WILLIAMS, M. C. *op. cit.* e SCHEUERMAN, W. Carl Schmitt and Hans Morgenthau: Realism and beyond. In: WILLIAMS, M. C. *op. cit.*

⁴⁹³ Com efeito, como nota Oliver Jüterssonke: “*the fact that Morgenthau came from the field of International Law is of no slight importance for an appreciation of his intellectual roots [...] Morgenthau's interactions with Lauterpacht and Kelsen form the basis for what would later become his realist theory of international politics*”. Cf. JÜTERSONKE, O. *op. cit.* In: WILLIAMS, M. C. *op. cit.* p. 94 e 99-100.

⁴⁹⁴ Como observa Scheuerman “*Herz, another German Jew forced to flee Nazism, was involved in émigré socialist politics during the 1930s. Morgenthau had been a leftleaning Weimar labor lawyer and protégé of Hugo Sinzheimer, the architect of the Weimar Constitution's expressly social democratic provisions. Although never a socialist, he at least sympathized briefly with core elements of an identifiably left-wing critique of capitalism*”. SCHEUERMAN, W. *op. cit.* p. 11. Vale dizer ainda que Morgenthau foi um incisivo crítico da Guerra do Vietnam e um árduo defensor do controle supranacional do arsenal nuclear dos Estados. Cf. MORGENTHAU, Hans J. “We Are Deluding Ourselves in Viet-Nam”, **New York Times Magazine**, 18 abr. 1965 e MORGENTHAU, H. J. Some Political Aspects of Disarmament In: CARLTON, David e SCHAEFER, Carlo [org.] **The Dynamics of the Arms Race**. Croom Helm, 1975.

⁴⁹⁵ Inclusive, sua produção acadêmica no pós-guerra ficou concentrada no estudo da revolução socialista soviética, do que resultou uma obra de quatorze volumes – *A History of Soviet Russia* publicados entre 1950 e 1978.

de que seus interesses são os mesmos da comunidade e seu colapso acarretaria o colapso da comunidade como um todo.^{496 497}

Se a retórica de padrões morais é na verdade a dissimulação de interesses de grupos dominantes, aspirações de paz e justiça universal deveriam ser vistas com suspeitas. Logo, Carr rejeita o caráter universal da moral, postulando sua natureza relativa e condicionando julgamentos éticos à Política.⁴⁹⁸ Segundo esse raciocínio, o equívoco central no projeto da Liga das Nações foi se basear na crença de que a manutenção do *status quo* político e territorial – o resultado de um cenário de paz – seria satisfatório para todas as grandes potências, algo improvável de ocorrer em um contexto de distribuição assimétrica do poder.⁴⁹⁹ De fato:

Assim como a classe dominante em uma comunidade clama por paz doméstica, que garanta sua própria segurança e predominância, e denuncia a guerra de classe, que pode ameaçá-la, a paz internacional se torna um interesse especialmente investido dos poderes predominantes.⁵⁰⁰

Como há Estados que são favorecidos pela paz e outros que são desfavorecidos pela manutenção desse *status quo*, o conflito entre eles, além de ser consequência da divergência ou da impossibilidade de estabelecimento de

⁴⁹⁶ “The doctrine of the harmony of interests thus serves as an ingenious moral device invoked, in perfect sincerity, by privileged groups in order to justify and maintain their dominant position. But a further point requires notice. The supremacy within the community of the privileged group may be, and often is, so overwhelming that there is, in fact, a sense in which its interests are those of the community, since its well-being necessarily carries with it some measure of well-being for other members of the community, and its collapse would entail the collapse of the community as a whole”. CARR, Edward Hallet. **The Twenty Years' Crisis 1919-1939: an introduction to the study of international relations**, 2 ed., Macmillan, 1946. p. 80.

⁴⁹⁷ Carl Schmitt sustentava um argumento semelhante ao tratar da manipulabilidade ideológica do conceito de humanidade: “When a state fights its political enemy in the name of humanity, it is not a war for the sake of humanity, but a war wherein a particular state seeks to usurp a universal concept against its military opponent. At the expense of its opponent, it tries to identify itself with humanity in the same way as one can misuse peace, justice, progress, and civilization in order to claim these as one's own and to deny the same to the enemy”. SCHMITT, Carl. **The Concept of the Political**: expanded edition. Tradução: George Schwab. The University of Chicago Press, [edição original: 1932], 2007. p. 54.

⁴⁹⁸ “Morality can only be relative, not universal. Ethics must be interpreted in terms of politics; and the search for an ethical norm outside politics is doomed to frustration”. CARR, E. H. op. cit. p. 21.

⁴⁹⁹ “The common interest in peace masks the fact that some nations desire to maintain the status quo without having to fight for it, and others to change the status quo without having to fight in order to do so. [...] The utopian assumption that there is a world interest in peace which is identifiable with the interest of each individual nation helped politicians and political writers everywhere to evade the unpalatable fact of a fundamental divergence of interest between nations desirous of maintaining the status quo and nations desirous of changing it”. *Ibidem*. p. 52-53.

⁵⁰⁰ “Just as the ruling class in a community prays for domestic peace, which guarantees its own security and predominance, and denounces class-war, which might threaten them, so international peace becomes a special vested interest of predominant Powers”. *Ibidem*. p. 82.

“verdades morais”, é também o resultado de políticas que almejam objetivos diversos. Nesse quadro, a Política é o único meio eficaz para dirimir os conflitos.

Na ótica realista, Política e poder são noções indissociáveis. Segundo Carr, “enquanto a política não pode ser satisfatoriamente definida exclusivamente em termos de poder, é seguro dizer que o poder é sempre um elemento essencial da política”.⁵⁰¹ Por consequência, Estados que possuem maior poder (não só militar, mas também econômico e político) são aqueles que efetivamente decidem as questões políticas mais relevantes. A conclusão parece simplória mas é utilizada por Carr para criticar a tentativa utópica de se, segundo ele, eliminar o poder da Política na Liga das Nações, o que ficou evidenciado pela pretensa igualdade formal entre seus membros.⁵⁰² Os Estados que efetivamente detêm o poder tendem a sustentar esse tipo de noção – o da separação entre poder e Política – para manter o *status quo* sem a necessidade de recorrer ao conflito com Estados mais fracos, que assim crêem possuir alguma influência política no rumo dos assuntos internacionais. Em um prognóstico preciso do que viria a se tornar o sistema de solução de controvérsias da ONU, Carr argumentou:

Uma vez que os Poderes insatisfeitos tenham percebido a possibilidade de remediar suas queixas por negociações pacíficas (sem dúvidas precedidas em primeira instância por ameaças de utilização da força), algum procedimento regular de “mudança pacífica” pode gradualmente ser estabelecido e ganhar a confiança dos insatisfeitos; e assim, uma vez que esse sistema tenha sido reconhecido, a conciliação iria ser considerada como o caminho normal, e a ameaça de utilização da força, enquanto nunca abandonada, recederia mais e mais para o segundo plano.⁵⁰³

É importante alertar, todavia, que o autor não defende o exercício cego do poder como instrumento de Política, relegando a moral à irrelevância como sugeria Maquiavel; pelo contrário, critica duramente teorias que postulam a separação entre

⁵⁰¹ “While politics cannot be satisfactorily defined exclusively in terms of power, it is safe to say that power is always an essential element of politics”. *Ibidem*. p. 102.

⁵⁰² “Utopian writers from the English-speaking countries seriously believed that the establishment of the League of Nations meant the elimination of power from international relations. [...] The assumption of the elimination of power from politics could only result from a wholly uncritical attitude towards political problems. In the affairs of the League of Nations, formal equality and the participation of all in debate did not render the power factor any less decisive”. *Ibidem*, p. 103-103.

⁵⁰³ “once the dissatisfied Powers had realised the possibility of remedying grievances by peaceful negotiations (preceded no doubt in the first instance by threats of force), some regular procedure of “peaceful change” might gradually be established and win the confidence of the dissatisfied; and that, once such a system had been recognised, conciliation would come to be regarded as a matter of course, and the threat of force, while never formally abandoned, recede further and further into the background”. *Ibidem*. p. 214.

Política e moral. Em suas próprias palavras: “A ação política deve ser baseada em uma coordenação de moralidade e poder. Essa verdade é de importância prática e teórica. Na política é fatal ignorar o poder tanto quanto o é a moralidade”.⁵⁰⁴

Atento a questões normativas, Carr se insurge contra a ideia de que o Direito é moralmente superior à Política ou que o Direito exerce um papel de “corretivo moral” aos “métodos imorais da Política”. Isso não significa que o Direito Internacional seja divorciado da moral ou mesmo que suas regras não possuam influência no comportamento dos Estados. Pelo contrário, Carr defende que o Direito confere à sociedade aquele elemento de regularidade e continuidade sem o qual a vida em sociedade não é possível⁵⁰⁵, daí se justificando seu caráter de obrigatoriedade.⁵⁰⁶ Logo, “O Direito Internacional é uma função da comunidade política das nações”.⁵⁰⁷

Não obstante, nota Carr que todo sistema jurídico pressupõe uma decisão política anterior sobre qual é a autoridade competente para legislar. Por isso conclui que a autoridade última da lei deriva da Política.⁵⁰⁸ Se no Direito Internacional a autoridade para legislar reside a princípio nos próprios destinatários da norma – os Estados – então a influência que recebe da Política é ainda maior que nos sistemas domésticos. Isso ficaria evidenciado na dificuldade de se desenvolver “regras gerais igualmente aplicáveis a todos” que segundo Carr é a base do elemento ético do Direito. Mesmo nesse caso, ainda que gerais em forma, se verificaria que essas regras:

[...] constantemente se dirigem a um Estado particular ou grupo de Estados; e por essa razão, se não por outra, o elemento poder é mais predominante e mais óbvio no Direito Internacional do que no doméstico, cujos sujeitos são um grande corpo de indivíduos anônimos.⁵⁰⁹

⁵⁰⁴ “Political action must be based on a coordination of morality and power. This truth is of practical as well as theoretical importance. It is as fatal in politics to ignore power as it is to ignore morality”. *Ibidem.* p. 97.

⁵⁰⁵ “Law gives to society that element of fixity and regularity and continuity without which no coherent life is possible”. *Ibidem.* p. 179.

⁵⁰⁶ “Law is regarded as binding because, if it were not, political society could not exist and there could be no law”. *Ibidem.* p. 177.

⁵⁰⁷ *Ibidem.* p. 178.

⁵⁰⁸ “Every system of law presupposes an initial political decision, whether explicit or implied, whether achieved by voting or by bargaining or by force, as to the authority entitled to make and unmake law. Behind all law there is this necessary political background. The ultimate authority of law derives from politics”. *Ibidem.* p. 180.

⁵⁰⁹ “The evolution of general rules equally applicable to all, which is the basis of the ethical element in law, becomes extremely difficult. Rules, however general in form, will be constantly found to be

Notando a ausência de um órgão legislativo internacional, característica da sociedade anárquica, bem como da dificuldade de se estabelecer algo do tipo – especialmente diante do fato de que a Liga das Nações estava longe de sê-lo – e expressando ceticismo com relação aos mecanismos de solução de controvérsias no Direito Internacional, em que não se verifica o elemento da jurisdição compulsória⁵¹⁰, Carr argumenta que é preciso analisar as condições de mudança social que não envolvam necessariamente a adoção de legislação.⁵¹¹ Uma dos meios de promover tal mudança seria através da ameaça de utilização da força, que o autor considera “uma condição necessária de importantes mudanças políticas na esfera internacional”⁵¹² – uma assertiva que precisa ser interpretada segundo o contexto histórico em que foi escrita. De fato, Carr somente defende a legitimidade da ameaça de utilização da força entre Estados após constatar que as restrições que a ela existem a nível doméstico não se repetiam naquele momento no Direito Internacional.⁵¹³ Ora, se a justificativa para a possibilidade de se recorrer à ameaça de utilização da força residia, segundo o autor, na ausência de proibição na normativa internacional, pode se inferir que, caso houvesse – como de fato hoje há – Carr certamente alcançaria conclusão contrária.

Todavia, observa o autor, os mecanismos de solução pacífica baseados no poder – cujo desenvolvimento seria o problema fundamental da política

aimed at a particular state or group of states; and for this reason, if for no other, the power element is more predominant and more obvious in international than in municipal law, whose subjects are a large body of anonymous individuals”. Ibidem. p. 178.

⁵¹⁰ *Ibidem.* p. 195.

⁵¹¹ “we may therefore find some help in the conception [...] of changes peacefully effected in the social structure without legislation or any other overt form of state intervention. Even to-day, it is easy to exaggerate the role of legislation; and it may still be true to say (as it would certainly have been true a hundred years ago) that the most important changes in the structure of society and in the balance of forces within it are effected without legislative action. It may be unnecessarily pessimistic to rush into the conclusion that the absence of an international legislature rules out any international procedure of peaceful change”. *Ibidem.* p. 212.

⁵¹² “Normally, the threat of war, tacit or overt, seems a necessary condition of important political changes in the international sphere”. *Ibidem.* p. 216.

⁵¹³ Carr observa que internamente os Estados democráticos contam com procedimentos legislativos que asseguram a mudança e a força do Estado para assegurá-la. Logo, “Thanks to these checks, a certain moral discredit attaches in democratic countries, in the minds of all classes, to the open use or threat of force until other means have been tried of bringing about a change. In international politics neither of these checks exists”. *Ibidem.* p. 215-216. Anteriormente o autor observa que mesmo o Pacto Kellogg-Briand não proibia a ameaça de utilização da força entre as partes mas apenas prescrevia a renúncia à guerra como instrumento de política nacional em suas relações. *Ibidem.* p. 171-172. Da mesma forma, a Convenção da Liga das Nações não previa qualquer proibição da ameaça ou utilização da força.

internacional⁵¹⁴ – não podem ser exercidos sem observância à moral; deve-se encontrar um meio de basear sua operação em um “um compromisso entre poder e moralidade, que é a fundação de toda vida política”.⁵¹⁵ A própria visão que Carr tem de uma política realista é moderada e busca afastar radicalizações⁵¹⁶, sob o reconhecimento de que uma “ordem internacional não pode ser baseada apenas no poder, pela simples razão de que a humanidade iria, no longo prazo, sempre se revoltar” contra o poder despido de moralidade.⁵¹⁷ Dessa forma:

O utopista que sonha que é possível eliminar auto-afirmação da política e basear o sistema político na moralidade apenas é tão equivocado quanto o realista que acredita que o altruísmo é uma ilusão e que toda ação política é baseada em egoísmo.⁵¹⁸

Em essência, a argumentação de Carr é um ataque aos projetos (utópicos) idealistas de manutenção da paz que não consideravam a importância que a distribuição do poder entre os Estados tem na forma como se relacionam. Manter a paz através da tentativa de exclusão do poder da Política Internacional seria uma empreitada fútil pois Estados desfavorecidos na balança de poder não se conformariam com a manutenção de tal *status quo*. Nesse cenário, os mecanismos formais de mudança, especialmente o Direito Internacional e a Liga das Nações, não se mostravam eficazes para assegurar a paz, daí a necessidade de se recorrer a formas alternativas de mudança pacífica. Isso não implica o argumento de que o Direito Internacional não é apto a fazê-lo mas apenas que a forma como os idealistas dele se utilizavam, sem atenção ao elemento poder, se mostravam ineficazes, o que ficou especialmente revelado no fracasso da Liga.

⁵¹⁴ *Ibidem*. p. 222.

⁵¹⁵ [...] if an orderly procedure of peaceful change is ever to be established in international relations, some way must be found of basing its operation not on power alone, but on that uneasy compromise between power and morality which is the foundation of all political life”. *Ibidem*. p. 220.

⁵¹⁶ “pure realism can offer nothing but a naked struggle for power which makes any kind of international society impossible” *Ibidem*. p. 93.

⁵¹⁷ “an international order cannot be based on power alone, for the simple reason that mankind will in the long run always revolt against naked power”. *Ibidem*. p. 236.

⁵¹⁸ “The utopian who dreams that it is possible to eliminate selfassertion from politics and to base a political system on morality alone is just as wide of the mark as the realist who believes that altruism is an illusion and that all political action is based on self-seeking”. *Ibidem*. p. 97.

5.1.2 Hans Joachim Morgenthau

Durante a ascensão do regime nazista na Alemanha muitos intelectuais judeus europeus se refugiaram na América, dentre eles Hannah Arendt, Leo Strauss, John Herz, Henry Kissinger e o próprio Hans Kelsen. Da mesma forma, Hans Morgenthau, quem chega aos Estados Unidos em 1937 e onde escreve importantes obras como *Scientific Man Versus Power Politics* (1946) e *Politics among Nations* (1948) – esta última seguramente uma das mais influentes teorias das Relações Internacionais.

Segundo Koskeniemi, da contradição entre a tradicional e idealista abordagem puramente sociológica das relações internacionais própria da literatura norte-americana, de um lado, e o excessivo formalismo jurídico germânico, de outro, Morgenthau elabora sua teoria.⁵¹⁹ O propósito da obra, assim diz o próprio Morgenthau em linhas introdutórias, é “detectar e entender as forças que determinam as relações políticas entre as nações, e compreender as formas de que essas forças atuam sobre cada uma delas e sobre as relações políticas e instituições internacionais”,⁵²⁰ bem como compreender “o problema da paz internacional”.⁵²¹

Assim como Carr, Morgenthau observa o vínculo essencial entre Política e poder; mas de forma mais enfática que aquele, argumenta que Política, seja ela doméstica ou internacional, é uma *luta por poder*. Define poder político como “as relações mútuas de controle entre os titulares da autoridade pública e entre estes e o povo em geral”⁵²², relações estas que possuem natureza psicológica entre aquele que exerce o poder e aquele sobre o qual o poder é exercido. Dessa forma, o poder se manifesta, afirma Morgenthau, como influência sobre as ações do outro, através de ordens, ameaças, persuasão ou uma combinação desses fatores.⁵²³

⁵¹⁹ “Morgenthau’s influence as the founder of international relations follows from his conscious departure from (legal) formalism on the one hand, but, crucially, of his steadfast refusal to collapse the field into mainstream sociology or ethics, on the other. He did not found the discipline despite the contradiction between realism and idealism in *Politics among Nations*. He founded it on that contradiction”. KOSKENIEMI, M. **The Gentle...** op. cit. p. 465.

⁵²⁰ “[...] to detect and understand the forces which determine political relations among nations, and to comprehend the ways in which those forces act upon each other and upon international political relations and institutions”. MORGENTHAU, Hans J. **Politics among Nations: the struggle for power and peace**. Alfred A. Knoff, 1948. p. 3.

⁵²¹ *Ibidem*. p. 7.

⁵²² “By political power we refer to the mutual relations of control among the holders of public authority and between the latter and the people at large”. *Ibidem*. p. 13.

⁵²³ “Political power is a psychological relation between those who exercise it and those over whom it is exercised. It gives the former control over certain actions of the latter through influence which the

É possível, sustenta o autor, que o objetivo remoto de determinada política seja relacionado à busca por liberdade, segurança, prosperidade, ou que suas metas sejam definidas em termos religiosos, filosóficos, econômicos ou sociais, mas o objetivo imediato sempre estará ligado ao ganho, manutenção ou demonstração de poder.⁵²⁴ Essa visão reducionista é inspirada pela crença de que as forças que moldam uma sociedade se encontram no senso de autopreservação e dominação do homem, e por consequência, de suas associações.⁵²⁵

Ocorre que se a luta por poder é domesticamente controlada pela estrutura hierárquica da autoridade estatal, favorecida por outros elementos de coesão social tais como a uniformidade cultural, internacionalmente as possibilidades de conflito são maiores na ausência desses elementos. De fato, constatou Morgenthau que “A história das nações ativas na política internacional as mostra continuamente se preparando para, ativamente envolvidas em, ou se recuperando de violência organizada em forma de guerra”.⁵²⁶ Nesse contexto, as formas de exercício da política internacional perante a *manutenção*, *aquisição* ou *demonstração* de poder revelam, respectivamente, uma *política de manutenção do status quo*, uma *política imperialista* e uma *política de prestígio*.⁵²⁷ Estabelecida tal categorização, Morgenthau analisa as condições que determinam a escolha de um ou outro tipo de política, os métodos empregados para exercê-las e as medidas apropriadas para responder a elas, especialmente a política imperialista.

former exert over the latter's minds. That influence may be exerted through orders, threats, persuasion, or a combination of any of these". Ibidem. p. 14.

⁵²⁴ “International politics, like all politics, is a struggle for power. Whatever the ultimate aims of international politics, power is always the immediate aim. Statesmen and peoples may ultimately seek freedom, security, prosperity or power itself. They may define their goals in terms of a religious, philosophic, economic, or social ideal. [...] But whenever they strive to realize their goal by means of international politics, they do so by striving for power”. *Ibidem. p. 13.*

⁵²⁵ “The drives to live, to propagate, and to dominate are common to all men” [...] “The desire to dominate, in particular, is a constitutive element of all human associations”. *Ibidem. p. 17.*

⁵²⁶ “The history of the nations active in international politics shows them continuously preparing for, actively involved in, or recovering from organized violence in the form of war”. *Ibidem. p. 21.*

⁵²⁷ Morgenthau categoriza os fenômenos políticos em três tipos básicos: “All politics, domestic and international, reveals three basic patterns, that is to say, all political phenomena can be reduced to one of three basic types. A political policy seeks either to keep power, to increase power, or to demonstrate power”. *Ibidem. p. 21-22.* É importante observar que pequenos ajustes na balança de poder não revelam uma mudança da política de manutenção do *status quo* para uma política imperialista. Morgenthau cita como exemplo a aquisição do território do Alasca pelos Estados Unidos em 1867. Segundo ele, o fato não representou uma mudança no *status quo* frente à Rússia pois com a tecnologia militar e de comunicações existente à época, a aquisição daquele então inacessível território não representava qualquer alteração na distribuição de poder entre os dois países.

Num cenário em que as relações entre os Estados são em essência relações de poder e em que objetivos diversos com relação à configuração que essas relações devam assumir sinalizam a permanente possibilidade de conflito, qual seriam os meios necessários para a manutenção da paz? Segundo Morgenthau tal fim somente poderia ser atingido por meio de dois mecanismos: através do equilíbrio de poder⁵²⁸, de um lado, e de outro pela imposição de restrições normativas ao comportamento dos Estados (o Direito e a Moralidade Internacional e a opinião pública mundial).⁵²⁹ Como Morgenthau considera que nenhum desses mecanismos, da forma como operavam ao momento, era capaz de conter a luta pelo poder em termos pacíficos, ele passa a analisar os fatores que interferem no balanceamento de poder entre os Estados e as condições de seu equilíbrio, bem como a eficácia daquelas limitações normativas.

Argumenta Morgenthau que o equilíbrio é uma característica imprescindível à existência de todo sistema social: sem o estado de equilíbrio, um elemento do sistema ganha ascendência sobre os outros e pode vir a destruí-los. Sendo assim, o objetivo do equilíbrio é manter a estabilidade do sistema e, ao mesmo tempo, a preservação de cada um de seus elementos. Os meios empregados para manter tal equilíbrio consistem em permitir aos diferentes elementos que realizem suas tendências conflitantes até o ponto em que a tendência de um não seja forte o suficiente para superar a tendência dos demais, mas forte o suficiente para prevenir os demais de superar sua própria tendência.⁵³⁰

Após descrever e analisar as configurações que o equilíbrio de poder entre os Estados pode assumir, os métodos de interferir nesse equilíbrio e como avaliá-los politicamente, Morgenthau conclui que “o poder é um método rude e pouco confiável para limitar as aspirações por poder no cenário internacional”. Se as motivações por trás da luta pelo poder e os mecanismos através dos quais ele opera fosse tudo o

⁵²⁸ A expressão em inglês utilizada por Morgenthau é “*balance of power*”. O autor emprega a expressão tanto no sentido de atuação na distribuição do poder entre os Estados – algo como “balanceamento” – quanto no sentido de configuração dessa distribuição.

⁵²⁹ “*In a world whose moving force is the aspiration for power of sovereign nations, peace can be maintained only by two devices. One is the self-regulatory mechanism of the social forces which manifests itself in the struggle for power on the international scene, that is, the balance of power. The other consists of normative limitations upon that struggle in the form of international law, international morality, and world public opinion*”. *Ibidem*. p. 8-9.

⁵³⁰ “*it is the purpose of all such equilibriums to maintain the stability of the system without destroying the multiplicity of the elements composing it [...] The means employed to maintain the equilibrium consist in allowing the different elements to pursue their opposing tendencies up to the point where the tendency of one is not so strong as to overcome the tendency of the others, but strong enough to prevent the others to overcome its own*”. *Ibidem*. p. 126-127.

que se precisa saber sobre política internacional, argumenta Morgenthau, então o cenário internacional de fato lembraria o Estado de natureza descrito por Hobbes, governado exclusivamente por considerações de conveniência política como quis Maquiavel, onde o fraco estaria à mercê do forte e o poder seria o que efetivamente diria o que é direito.⁵³¹

Mas a sociedade internacional é dotada de mecanismos que operam para limitar os impulsos de dominação dos Estados quando o equilíbrio de poder se mostra deficiente. Seriam eles, segundo Morgenthau, a ética, os costumes e o Direito Internacional.

Quando uma sociedade ou alguns de seus membros são incapazes de se proteger por sua própria força contra os impulsos de poder de outros, quando, em outras palavras, a mecânica da política de poder se mostra deficiente, como cedo ou tarde acontece, os sistemas normativos tentam suplementar a política de poder com suas próprias regras de conduta. Essa é a mensagem que os sistemas normativos dão aos fortes e fracos: um poderio superior não dá direito, tanto moral quanto jurídico, a fazer com esse poder tudo que é fisicamente possível fazer. O poder é sujeito a limitações, no interesse da sociedade como um todo e no interesse de seus membros individualmente, que não são resultado da mecânica da luta pelo poder, mas sim superimpostas sobre essa luta na forma de normas ou regras de conduta pela vontade dos próprios membros da sociedade.⁵³²

Como se nota, Morgenthau considera a normativa internacional um corretivo aos mecanismos deficientes da balança de poder. Obviamente, nessa concepção se reconhece a capacidade do Direito Internacional de limitar o comportamento dos Estados. Essa passagem da obra mostra com clareza porque as críticas dirigidas a Morgenthau são muitas vezes injustificadas: exageram o papel que o poder tem em

⁵³¹ “power is a crude and unreliable method of limiting the aspirations for power on the international scene. If the motivations behind the struggle for power and the mechanisms through which it operates were all that needs to be known about international politics, the international scene would indeed resemble the state of nature described by Hobbes as a ‘war of every man against every man’. International politics would be governed exclusively by those considerations of political expediency of which Machiavelli has given the most acute and candid account. In such a world the weak would be at the mercy of the strong. Might would indeed make right”. *Ibidem*. p. 169.

⁵³² “When a society or certain of its members are unable to protect themselves with their own strength against the power drives of others, when, in other words, the mechanics of power politics are found wanting, as sooner or later they must, the normative systems try to supplement power politics with their own rules of conduct. This is the message the normative systems give to strong and weak alike: Superior power gives no right, either moral or legal, to do with that power all that is physically capable of doing. Power is subject to limitations, in the interest of society as a whole and in the interest of its individual members, which are not the result of the mechanics of the struggle for power, but are superimposed upon that struggle in the form of norms or rules of conduct by the will of members of society themselves”. *Ibidem*. p. 170

sua teoria realista e ignoram o valor que nela se atribui às regras de Direito e moralidade internacional.

Morgenthau reconhece que, “durante os quatrocentos anos de sua existência, o Direito Internacional tem sido, na maioria das vezes, escrupulosamente observado”.⁵³³ Todavia, existiam deficiências e limitações no Direito Internacional que prejudicavam sua plena eficácia na tarefa de correção do equilíbrio de poder. São problemas referentes à precariedade de suas funções legislativa, judicial e de execução das decisões (*enforcement*) – a primeira interessando particularmente à presente análise – quando comparadas aos sistemas jurídicos domésticos.

A primeira limitação inerente à função legislativa do Direito Internacional que identifica Morgenthau é relacionada ao seu caráter descentralizado. Na ausência de um órgão legislativo supranacional, a produção normativa do Direito Internacional se manifestava, segundo o autor, precipuamente por regras de caráter contratual, os tratados, cuja obrigatoriedade era dependente do consentimento de seus destinatários. O autor não ignora a existência das, segundo ele poucas, normas de Direito Internacional Geral, especialmente de caráter costumeiro, mas a preponderância dos tratados contratuais caracterizava um quadro fragmentado de regras entre Estados que estavam sujeitos a regimes diversos uns em relação aos outros, sobre uma só matéria. Utilizando a metáfora de Morgenthau, seria como uma cidade que tivesse uma lei para cada rua.⁵³⁴

É verdade que da época em que foi escrita a obra até o momento atual, a abrangência global da filiação à ONU permitiu que, da mesma forma, muitos tratados alcançassem a ratificação da maioria dos Estados. A evolução da concepção das normas *jus cogens* e das obrigações *erga omnes* também contribuiu para atenuar o cenário descrito por Morgenthau. Em contrapartida, o próprio movimento de globalização do Direito Internacional conduziu ao efeito paradoxal de *fragmentação*, ou seja, o surgimento de regimes especializados e relativamente autônomos em relação ao Direito Internacional Geral.⁵³⁵

⁵³³ *Ibidem.* p. 211.

⁵³⁴ *Ibidem.* p. 212.

⁵³⁵ Como observado no relatório da Comissão de Direito Internacional da ONU sobre o fenômeno da fragmentação do Direito Internacional: “*It is a well-known paradox of globalization that while it has led to increasing uniformization of social life around the world, it has also lead to its increasing fragmentation – that is, to the emergence of specialized and relatively autonomous spheres of social action and structure*”. UNITED NATIONS. Fragmentation of International Law: Difficulties Arising From the Diversification and Expansion of International Law. **International Law**

Um problema ainda mais grave decorrente da descentralização legislativa do Direito Internacional e do forte papel que o princípio do consentimento (ainda) tem na produção de suas normas reside na dificuldade de se regular assuntos em relação aos quais os Estados possuem interesses sensivelmente díspares. Como não há um órgão legislativo representativo que possa propor legislação nessas situações que absorva a divergência, os Estados são incapazes de concordar em termos de regras, de forma que “a insegurança e a confusão frequentemente reinam”.⁵³⁶ Tudo isso é agravado por problemas de interpretação das regras de Direito Internacional e de adjudicação e execução das decisões, em relação a que o autor apresenta detidas considerações que para os fins da presente análise não são tão relevantes quanto as críticas que são dirigidas à função legislativa.

É verdade que esses problemas sempre foram – e continuam a ser – reconhecidos e apontados por qualquer comentarista do Direito Internacional, seja ele um jurista ou um analista de política e relações internacionais. Não há quem os ignore. O que há de peculiar na crítica realista, nesse particular, é a associação das limitações do Direito Internacional com o exercício do poder dos Estados. São deficiências que geram incertezas e abrem caminhos para o abuso de poder. Como afirma Morgenthau, os governos

estão sempre ansiosos por livrar-se da influência restritiva que o Direito Internacional possa ter sobre sua política externa para, ao contrário, usar o Direito Internacional para a promoção de seus interesses nacionais, e para evadir obrigações legais que possam ser prejudiciais a eles. Eles têm usado a imprecisão do Direito Internacional como uma ferramenta feita sob medida para alcançar seus objetivos. Eles tem feito isso ao apresentar reivindicações legais mal fundamentadas sobre direitos jurídicos e ao distorcer o significado de regras de Direito Internacional reconhecidas em geral. Dessa forma, a falta de precisão, inerente à natureza descentralizada do Direito Internacional, gera ainda mais imprecisão e o vício debilitante, que está presente já em seu nascimento, continua a minar sua força.⁵³⁷

Commission, 2006. p. 11. Disponível em:
http://legal.un.org/ilc/documentation/english/a_cn4_l682.pdf

⁵³⁶ “Many matters bearing upon international relations, such as immigration and many aspects of economic policies, are not regulated by international law. The interests of the different nations in these matters are so divergent that they are unable to agree upon legal rules. In those matters with regard to which agreement was possible, insecurity and confusion frequently reign”. MORGENTHAU, H. J. **Politics**... op. cit. p. 212.

⁵³⁷ “Governments, however, are always anxious to shake off the restraining influence which international law might have upon their international policies, to use international law instead for the promotion of their national interests, and to evade legal obligations which might be harmful to them. They have used the imprecision of international law as a ready-made tool for furthering their ends.

Se as deficiências que viciam o Direito Internacional não forem sanadas e, por consequência, não for ele capaz de corrigir os mecanismos da balança de poder como um conjunto de proposições normativas que sejam de fato eficazes para limitar o comportamento dos Estados, então seu papel será o de “preencher uma função ideológica similar às políticas de *status quo*”. Se não for capaz de interferir significativamente na distribuição do poder como um mecanismo de mudança social, o Direito Internacional se resume a uma “força estática” de especial valor para Estados que desejam manter o *status quo*.⁵³⁸

5.1.3 John Herz

Em seu principal trabalho, *Political Realism and Political Idealism* (1951), John Herz define o realismo como o modo de pensar as relações internacionais em que se leva em consideração as implicações de fatores de segurança e poder, que seriam inerentes a toda sociedade. Em contraste, o idealismo político ignora ou, se considera estes fatores, o faz de forma superficial, concentrando em soluções ou condições racionais do desenvolvimento de um ideal que já está presente ou que seja realizável no futuro.⁵³⁹ Herz reconhece a existência de falhas e êxitos presentes nos dois modelos⁵⁴⁰ e a partir daí busca traçar uma teoria que se posiciona entre eles (“liberalismo realista”)⁵⁴¹, e por isso sua reunião com outros autores realistas é

They have done so by advancing unsupported claims to legal rights and by distorting the meaning of generally recognized rules of international law. Thus the lack of precision, inherent in the decentralized nature of international law, is breeding ever more lack of precision, and the debilitating vice, which was present at its birth, continues to sap its strength”. Ibidem. p. 214.

⁵³⁸ “The ideal of international law fulfills a similar ideological function for policies of status quo. Law in general and, especially, international law is primarily a static social force. It defines a certain distribution of power and offers standards and processes to ascertain and maintain it in concrete situations. Domestic law, through a developed system of legislation, judicial decision and law enforcement, allows for adaptations and sometimes even considerable changes within the general distribution of power. International law, in the absence of such a system making for lawful change, is [...] not only primarily, but essentially, a static force. The invocation of international law, of ‘order under law’, of ‘ordinary legal processes’ in support of a particular foreign policy, therefore, always indicates the ideological disguise of a policy of the status quo”. *Ibidem.* p. 64.

⁵³⁹ HERZ, John H. **Political Realism and Political Idealism**: a study in theories and realities. The University of Chicago Press, 2 ed., 1959. p. 18-19.

⁵⁴⁰ *Ibidem.* Capítulo 2.

⁵⁴¹ Explica Herz sobre esse “meio-termo”: “[...] we do not intend to suggest any unsystematic combination of certain elements of realism with certain other idealistic ones [...] We would do something different. We propose to take over from Political Idealism its basic ethical assumption as the yardstick and criterion of political of what ‘should be’, i. e., as the guiding criterion of political

feita com algumas qualificações. De um lado, é realista porque rejeita, assim como Carr e Morgenthau, o idealismo utópico de teorias liberais, preocupantemente distante dos fatos. Por outro lado, é liberalista no sentido de que reconhece a necessidade de orientar a ação política por valores morais humanísticos.

No que toca às proposições realistas da obra, destaca-se a elaboração da ideia do “dilema da segurança”, que forte influência exerceu sobre a evolução do pensamento realista que se seguiu. Num ambiente anárquico de competição, os Estados e seus líderes acumulam poder por razões de segurança, o que provoca o sentimento de insegurança em outros Estados; isso leva estes a reunir poder pelas mesmas razões mas agrava o propósito inicial de segurança daqueles. Segundo Herz:

Grupos politicamente ativos e indivíduos estão preocupados com sua segurança por poderem ser atacados, subjugados, dominados ou aniquilados por outros grupos e indivíduos. Porque eles lutam para obter segurança contra tais ataques e, ainda assim, nunca podem se sentir totalmente seguros em um mundo de unidades competidoras, eles são levados a adquirir mais e mais poder, de forma a escapar do impacto do poder superior de outros. É importante perceber que tal competição por segurança e, conseqüentemente, por poder, é uma situação básica e única entre os homens e seus grupos sociais.⁵⁴²

Adiante, reforçando a mesma ideia:

O Realismo Político [...] sempre concentra em torno do dilema básico que surge do próprio fato da competição humana por segurança, nomeadamente, o círculo vicioso da competição que nunca alcança segurança plena, mas que, ao tentar fazê-lo, aumenta a necessidade de acumular poder como um meio de obter mais segurança.⁵⁴³

O dilema da segurança enfatiza o aspecto de incerteza e desconfiança nas relações internacionais: confrontados com o imperativo de sobrevivência e

aims and action. But we also propose to utilize, without compromise or euphemism, any and all knowledge and insight which Political Realism possesses". Ibidem. p. 133.

⁵⁴² *"politically active groups and individuals are concerned about their security from being attacked, subjected, dominated, or annihilated by other groups and individuals. Because they strive to attain security from such attack, and yet can never feel entirely secure in a world of competing units, they are driven toward acquiring more and more power for themselves, in order to escape the impact of the superior power of others. It is important to realize that such competition for security, and hence for power, is a basic situation which is unique with men and their social groups". Ibidem. p. 14.*

⁵⁴³ *"Political realism [...] always centers around the basic dilemma which arises from the very fact of human competition for security, namely, the vicious circle of competition which never quite achieves full security, but which, in trying to do so, increases the necessity for accumulating power as a means of attaining more security" Ibidem. p. 24.*

incapazes de saber com absoluta certeza quais as intenções dos rivais, indivíduos e grupos sociais tendem a suspeitar uns dos outros. Isso os motiva a acumular poder para reforçar sua segurança.⁵⁴⁴

Se concordam com a proposição de Herz de que a segurança é o principal motivador dos Estados em um ambiente anárquico⁵⁴⁵, os realistas vão divergir sobre qual a melhor forma de se obter tal segurança. Dessa divergência surge a distinção entre o “realismo defensivo” e o “realismo agressivo” ou “ofensivo”.⁵⁴⁶ Extrapolando os limites da análise do realismo clássico, argumenta-se na vertente *defensiva* que a maneira mais eficaz de se obter segurança é através da formação de alianças defensivas.⁵⁴⁷ Já a variante *ofensiva* do neorrealismo, atualmente protagonizada por John Mearsheimer, interpreta o dilema da segurança como um propulsor à dominação: “o melhor meio para um Estado sobreviver na anarquia é levar vantagem sobre outros Estados e ganhar poder às suas custas. A melhor defesa é um bom ataque”.⁵⁴⁸ Isso não significa, na leitura ofensiva, que Estados se lancem a agressões como regra. Os fatos mostram o contrário. É que eles calculam em termos de equilíbrio de poder sobre como os outros Estados iriam reagir às suas ações, avaliando custos e riscos de uma política ofensiva.⁵⁴⁹

Tal como Morgenthau, Herz concebe o equilíbrio de poder como uma atenuante ao ambiente anárquico internacional. Como um tipo especial de “política de poder” (*power politics*), os mecanismos do equilíbrio se opõem a um cenário em que Estados se rivalizam cegamente para tentar dominar e subjugar uns aos outros.⁵⁵⁰ Mas é preciso distinguir entre um equilíbrio de poder espontâneo e o

⁵⁴⁴ Como afirma William Scheuerman: “Faced with the imperative of survival, and burdened with the knowledge that others easily posed threats while never being able to know for sure what potential rivals might intend, individuals and social groups were likely to be suspicious of others. Consequently, they possessed strong incentives to accumulate power resources in order to guarantee security”. SCHEUERMAN, W. *op. cit.* p. 34.

⁵⁴⁵ “In anarchy, security is the highest end. Only if survival is assured can states safely seek such other goals as tranquility, profit, and power”. WALTZ, K. N. **Theory of International Politics**. Addison-Wesley, 1979. p. 126.

⁵⁴⁶ Tal distinção foi originalmente proposta em SNYDER, Jack. **Myths of Empire: Domestic Politics and International Ambition**. Cornell University Press, 1991. p. 12.

⁵⁴⁷ Como representantes da variante defensiva do realismo: WALT, Stephen M. **The Origins of Alliances**, Cornell University Press, 1990 e SNYDER, J. *op. cit.*

⁵⁴⁸ “the best way for a state to survive in anarchy is to take advantage of other states and gain power at their expense. The best defense is a good offense”. MEARSHEIMER, J. J. *op. cit.* p. 43.

⁵⁴⁹ *Ibidem.* p. 44-45.

⁵⁵⁰ “‘balance of power policy’ is one type – a particular and particularly refined one – of power politics. On the other hand, it constitutes a type of policy which deviates from, and is opposed to, the entirely unregulated play of power politics, in which the respective units strive blindly, and without any system or common rules, to dominate and subjugate other units”. HERZ, J. H. *op. cit.* p. 206.

consciente. No primeiro caso, o equilíbrio é resultado de uma distribuição não-controlada de poder em que um certo número de Estados apresenta níveis equiparáveis de poder que os impedem de subjugar uns aos outros. Tal situação, explica Herz, ocorre quase que “naturalmente”, sempre que uma potência não se mostra forte o suficiente para destruir outra sem provocar a resistência dos demais Estados que, combinada, é capaz de resistir à sua força.⁵⁵¹

Diversamente, um cenário de equilíbrio “consciente” é caracterizado por um sistema que é politicamente determinado. Nesse caso, os responsáveis pela condução da política externa de algumas potências deliberadamente organizam suas políticas de forma a preservar o equilíbrio de poder e, se necessário for, a defesa e restauração desse equilíbrio. Observa Herz que esse sistema não previne guerra ou “pressões” que seriam “medidas necessárias” para manter ou restaurar o equilíbrio quando ameaçado por tendências hegemônicas. A vantagem desse sistema – longe de ser perfeito, mas melhor que a completa anarquia – é o de evitar que uma potência ou grupo hegemônico seja apto a oprimir e subjugar os demais Estados. Portanto, conclui Herz, que a política de equilíbrio de poder é uma peculiar combinação de políticas de poder individualistas, motivadas por interesses egoísticos, e um tipo de política de “interesse geral” que mutuamente se beneficia de um sistema de equilíbrio em que seus membros podem coexistir.⁵⁵²

5.2 Análise realista das possibilidades regulatórias da espionagem internacional

Como se pôde notar do contato com os principais argumentos dos autores realistas clássicos, as críticas que recebe o pensamento realista como um todo são em boa parte desmerecidas, fruto de uma caricaturização superficial e irrefletida de suas proposições. O realismo pronunciado por aqueles autores não relega à futilidade o Direito e a moralidade como instrumentos inaptos a influenciar o comportamento dos Estados; pelo contrário, reconhece a necessidade de

⁵⁵¹ “A balance or equilibrium of power may be merely the mechanical result, so to speak, of a situation in which a number of powers are so equal in power that they are unable to subjugate each other, the mere fact of their relative equality thus guaranteeing their continued existence as independent units alongside each other. Such a situation develops almost “naturally” whenever one power proves too weak to destroy the next strongest one without provoking the successful resistance of all the other units, which, combined, are capable of resisting its might”. *Ibidem*. p. 206.

⁵⁵² *Ibidem*. p. 207-208.

observância de regras como um corretivo aos mecanismos de distribuição do poder na sociedade internacional. Ocorre que limitações e deficiências identificadas no Direito Internacional impedem sua realização como um mecanismo eficaz de mudança, reduzindo-o a mais um dos instrumentos que os Estados mais poderosos têm a sua disposição para a manutenção do *status quo*.

É verdade, como já foi dito, que todas essas deficiências são reconhecidas na literatura do Direito Internacional. Qualquer jusinternacionalista reconhece a estrutura descentralizada das funções legislativa e judicial do Direito Internacional e aqueles que se propõem a refletir sobre as relações entre Política e Direito irão notar o forte papel que o fator “poder” exerce na criação, adoção e aplicação de suas regras. A esse propósito, vale ser transcrita uma ponderação de Oscar Schachter – que, se analisada com cuidado, ressoa argumentos realistas de Morgenthau:

O Direito Internacional deve também ser visto como o produto de uma experiência histórica em que o poder e a “relação de forças” são determinantes. Aqueles Estados com poder (*i.e.* a habilidade de controlar resultados contestados por outros) irão ter uma desproporcional e por vezes decisiva influência em determinar o conteúdo das regras e sua aplicação na prática. Por ser esse o caso, o Direito Internacional, em um sentido amplo, tanto reflete quanto sustenta a ordem política existente e a distribuição do poder.⁵⁵³

Se se identifica e reconhece abertamente os problemas do Direito Internacional, sua associação com o realismo político torna-se perfeitamente adequada do ponto de vista lógico. É preciso reconhecer, nas palavras de Malcolm Shaw – que surpreenderia a muitos por sua sintonia com Carr – que “é um erro assim como impreciso pedir do direito internacional mais do que ele pode entregar”⁵⁵⁴; ele não pode ser uma fonte de soluções instantâneas para conflitos em razão de sua “inerente fraqueza em estrutura e conteúdo”. Falhar em reconhecer tais limitações encoraja uma abordagem utópica divorciada da realidade. Por outro lado, a “atitude cínica com obsessão pelo poder bruto é igualmente imprecisa”. Entre os

⁵⁵³ “International law must also be seen as the product of historical experience in which power and the “relation of forces” are determinants. Those States with power (*i.e.*, the ability to control the outcomes contested by others) will have a disproportionate and often decisive influence in determining the content of rules and their application in practice. Because this is the case, international law, in a broad sense, both reflects and sustains the existing political order and distribution of power”. SCHACHTER, Oscar. General Course in Public International Law. **Collected Courses of the Hague Academy of International Law**, 1982. p. 28.

⁵⁵⁴ “it is a mistake as well as inaccurate to claim for international law more than it can possibly deliver”. SHAW, M. N. *op. cit.* p. 7.

vícios e virtudes do Direito Internacional, saber o que ele pode realizar e o que ele não pode oferece o melhor caminho.⁵⁵⁵

Paralelamente a essa tônica realista de cautela, moderação e até mesmo certo ceticismo perante o Direito Internacional, o realismo político oferece uma estrutura repleta de proposições para se pensar o problema do poder nas relações internacionais: suas formas de exercício, as condições e os mecanismos de sua configuração equilibrada, a natureza competitiva do ambiente anárquico e as proposições do dilema da segurança.

Uma vez estabelecida essa breve releitura do realismo clássico, cabe agora analisar como seus argumentos ajudam a entender a tolerância da espionagem internacional. Para tanto, sugerem-se as seguintes premissas teóricas:

a) *Qualquer grau e espécie de regulação jurídica implica diminuição de liberdade de atuação.* Se os Estados exercem a espionagem em um ambiente de tolerância jurídica e política da atividade há um certo grau de liberdade que seria reduzido em caso de eventual regulação. Em outras palavras, regular o exercício da espionagem internacional significaria inevitavelmente restringir suas possibilidades de realização. Realmente, ainda que tal regulação hipotética possibilitasse amplas margens de atuação, ela nunca seria tão extensa quanto a própria liberdade (recorde-se a distinção entre direito e liberdade feita na seção 4.5.1), caso contrário não seria nem mesmo necessário regular a atividade.

b) *Obtenção de informação implica acréscimo de poder.* A relevância da informação obtida irá determinar o grau do ganho em poder e o seu tipo irá determinar se houve um acréscimo ao poderio militar, econômico ou político do Estado coletor. Já *um ganho em capacidade de inteligência implica um ganho potencial de poder.* Diz-se “potencial” porque, não sendo a inteligência um fim em si mesmo, valendo ela tanto quanto sua eficiência em obter informação, sua capacidade apenas representa, em maior ou menor grau, uma possibilidade de coleta. Por outro lado, a *perda em capacidade de inteligência resulta em perda efetiva de poder* pois ou as possibilidades de coleta de informação presentes serão

⁵⁵⁵ “International law cannot be a source of instant solutions to problems of conflict and confrontation because of its own inherent weaknesses in structure and content. To fail to recognise this encourages a utopian approach which, when faced with reality, will fail. On the other hand, the cynical attitude with its obsession with brute power is equally inaccurate, if more depressing. It is the medium road, recognising the strength and weakness of international law and pointing out what it can achieve and what it cannot, which offers the best hope”. SHAW, M. N. op. cit. p. 12-13.

diretamente afetadas ou o potencial ganho de poder que contrariamente seria adquirido com o aumento da capacidade será virtualmente anulado.

Vale ainda ser feita uma observação a respeito do *conceito de poder*. Os autores realistas a quem se recorre neste trabalho não apresentam uma definição precisa do que consideram que se deva entender por “poder”. Morgenthau, por exemplo, em *Politics among Nations*, utiliza o termo em sentido amplo e variável, ora significando controle/influência, ora força/capacidade.⁵⁵⁶ A falta de um conceito delimitado de poder também se repete nesta tese, mas não prejudica a compreensão e a validade da argumentação. Aqui se sugere um sentido próximo à força/capacidade quando se fala em “resultante de poder” ou relações de ganho e perda de poder, transmitindo uma ideia de poder como uma expressão dos recursos materiais do Estado (poder político, econômico, militar ou o próprio poder de inteligência).

Fixadas tais premissas, discute-se a seguir como eventuais pretensões regulatórias à espionagem internacional seriam desacreditadas pelas próprias características inerentes à atividade e por afetar interesses vitais de poder e segurança dos Estados:

5.2.1 *Alto custo de eventual fracasso das negociações*

Inicialmente, a própria mobilização dos Estados para ingressar em negociações sobre a regulação internacional da atividade já sinalizaria dificuldades tamanhas o suficiente para desmotivar o início do processo. Isso porque, qualquer discussão a nível internacional sobre um acordo de limitação da espionagem, para ter um resultado efetivo, exigiria que os Estados revelassem informações sensíveis sobre suas próprias capacidades de inteligência. Os Estados precisariam “sentar à mesa de negociação” com uma certa disposição à transparência, mostrando ao menos algumas particularidades de seu serviço de inteligência que comporiam o espectro da regulação – que obviamente seriam informações classificadas. As partes precisam saber o que realmente é necessário limitar para que assim o acordo possa ter algum valor.

⁵⁵⁶ Como observa Yan Xuetong em XUETONG, Y. *op. cit.* p. 5. O autor ainda explica que no idioma chinês existem termos diferentes para as duas concepções de poder, sendo “*quanli*” para se referir a poder de controle/influência política e “*shili*” para força/capacidade.

Isso não seria problema se as negociações tivessem êxito, terminando no ajuste de um tratado de limitação da espionagem entre todas as partes envolvidas, pois aquilo que fosse revelado por elas sobre suas capacidades de inteligência seria absorvido pela regulação. Entretanto, se frustradas as negociações, informações classificadas teriam sido reveladas a troco de nada. Os representantes dos Estados retornariam aos seus respectivos países com informações sobre o aparato de inteligência dos demais Estados, de forma que aquele que tivesse revelado mais – ou seja, aquele Estado que estivesse comprometido com a transparência em maior grau – seria o que suportaria o maior prejuízo em termos de poder. O mesmo vale se considerarmos que não há qualquer garantia de que, mesmo em caso de sucesso nas negociações que culminem com a aprovação de um texto, todos os Estados posteriormente venham a ratificar o tratado.

É verdade que essa perda de poder resultante da revelação espontânea de algumas informações referentes à inteligência estatal seria apenas marginal e corrigida ao longo do tempo. De fato, mesmo que ingressando em negociações dessa natureza de boa-fé, os Estados por certo não revelariam suas informações de maior relevância estratégica e, mesmo no caso de fracasso nas negociações, aquelas facetas de suas operações ou capacidades que fossem objeto da revelação seriam posteriormente substituídas na estrutura de sua inteligência, anulando assim o pequeno ganho de poder dos outros Estados.

Isso sugere ainda um outro problema: como saber que as informações que os Estados trazem à mesa de negociações são realmente verdadeiras? Como atestar que um Estado negocia de boa-fé se não se sabe com antecedência exatamente qual é a sua capacidade de inteligência dada a natureza classificada dessa informação. Mesmo que se saiba, essa informação necessariamente teria sido obtida pela espionagem, o que conduz a um problema cíclico: se, por exemplo, Estados Unidos e China iniciam negociações com a finalidade de eliminar a condução de espionagem econômica entre eles, ambos os Estados somente podem saber se o outro age de forma transparente nas negociações se previamente tiverem obtido informações sobre a capacidade de inteligência do outro, o que é feito através da própria espionagem.

Obviamente, os Estados que pretendam negociar um tal acordo podem simplesmente ignorar detalhes específicos sobre a capacidade de inteligência de cada uma das partes envolvidas e se comprometerem a uma proibição genérica do

exercício da espionagem. Nesse caso, o custo em termos de poder de eventual fracasso nas negociações seria anulado. Todavia, um acordo em linhas genéricas de proibição certamente se revelaria deficiente em termos de eficácia, pois dúvidas surgiriam quanto a o que exatamente se deveria entender por “espionagem” e em que condições sua prática seria admissível – por exemplo, em situações de beligerância ou por razões de segurança nacional. Se se desejasse ingressar a tal nível de detalhamento, então o propósito de generalização teria de ser abandonado, se tornando mais difícil manter questões sobre a capacidade individual de inteligência dos Estados fora das negociações.

Em conclusão, como se nota, diante da remota possibilidade de se alcançar a aprovação de um acordo de limitação da espionagem, os Estados provavelmente sequer ingressariam em negociações a respeito.

5.2.2 *Limitações à promoção da segurança e ao poder*

Mesmo que tais desconfiças e incertezas fossem superadas, as chances de que um Estado voluntariamente se sujeite a limitações à sua segurança e redução de poder relativo são muito baixas. De fato, a coleta de informações privadas irá permitir a identificação e vigilância de indivíduos que possuem ligações com grupos terroristas que operem em seu território e, eventualmente, até o desmantelamento de células terroristas. Informações políticas e militares permitirão acompanhar intenções e preparações hostis de Estados inimigos – seja internamente ou externamente à embaixadas e bases militares – além de possibilitar monitorar o cumprimento de acordos ou a conformidade com sanções que limitem a capacidade bélica de outro Estado, especialmente nuclear.

A situação da Coreia do Norte é a que atualmente melhor ilustra a importância da espionagem de segredos de Estado. Considerado um dos países mais fechados do mundo ao acesso estrangeiro, o regime comunista ditatorial conta apenas com a China como real aliado – muito embora tenha havido um distanciamento de Pequim nos últimos anos – e possui como seu maior trunfo a posse de armas nucleares. Declaradamente inimiga do vizinho sul, Japão e Estados Unidos, o nível de hostilidade da Coreia do Norte tem crescido ao longo do ano de 2016, em que se assistiu à realização de diversos testes balísticos e atômicos, inclusive a maior detonação de um dispositivo nuclear em sua história, no mês de setembro daquele

ano.⁵⁵⁷ Nesse ambiente, os riscos de um ataque surpresa são reais e consideráveis. Por essa razão, é necessário manter um aparato de monitoração constante sobre as atividades militares e políticas do país para que seja possível antecipar um ato de agressão de consequências catastróficas para a manutenção da paz. Isso pode ser feito através de sensores, satélites direcionados para seu território, espiões posicionados em setores sensíveis do governo e intrusões cibernéticas nos sistemas de defesa.

Perante uma ameaça de tal ordem, por que então um Estado ajustaria voluntariamente limitações à sua capacidade de descobrir riscos presentes ou potenciais à sua segurança – na ótica realista o valor supremo em um Estado? Uma possível resposta seria a de que, ao aceitar limitar o exercício de sua própria espionagem, o Estado se beneficiaria pela limitação também das atividades dos demais, estando assim seus segredos mais protegidos, portanto. Esse argumento seria falho pois ignora a constatação básica de que os Estados têm diferentes níveis de capacidade de condução de atividades de inteligência. Enquanto países como Estados Unidos, Reino Unido, Rússia, China e Israel, para citar apenas alguns exemplos, possuem larga capacidade de coleta de informações – alguns mais eficientes no exercício da HUMINT outros em SIGINT – outros países são bastante limitados na tarefa.

Logo, os Estados que contam com maiores recursos para o exercício da inteligência – que segundo as premissas antes estabelecidas significa contar com maior poder – se verão desmotivados a contrair voluntariamente limitações a sua capacidade de condução de atividades de inteligência, pois a própria realidade já determina essa limitação aos demais Estados. Segundo a concepção realista, o que interessa, portanto, aos Estados mais poderosos em termos de capacidade de inteligência é a simples manutenção do *status quo* como resultado da tolerância da espionagem internacional. Com efeito, se os Estados avaliam os resultados de suas políticas e ações em termos relativos – outra premissa realista – apenas aos Estados de menor capacidade de inteligência haveria interesse em estabelecer um parâmetro restritivo de condução da atividade, pelo que reduziriam um pouco da assimetria que os distancia das grandes potências da inteligência.

⁵⁵⁷ NORTH Korea's 'biggest' nuclear test sparks global outrage. **BBC News**, 9 set. 2016. Disponível em: <<http://www.bbc.com/news/world-asia-37317782>>

Seria possível sustentar contra esse argumento, por analogia, que a proibição genérica do uso da força na Carta da ONU⁵⁵⁸ foi ajustada mesmo num contexto em que os Estados possuíam diferentes capacidades militares, ou seja, num cenário de distribuição heterogênea do poder. Logo, seguiria o raciocínio, a espionagem poderia ser igualmente proibida entre Estados que contam com diferentes níveis de capacidade de exercício da inteligência. Verificar a validade dessa proposição nos leva à pergunta do porquê os Estados mais poderosos aceitaram se sujeitar a um regime rígido de proibição da utilização da força ao final da Segunda Guerra Mundial. A resposta reside no peculiar funcionamento do sistema de segurança coletiva da ONU.

Ao final do conflito, os vencedores (Estados Unidos, Reino Unido, França, União Soviética e China) somente aceitaram a mesma constrição à utilização da força que limitaria os Estados mais fracos porque foram investidos de duas prerrogativas que compensaram tal limitação: uma representação permanente no Conselho de Segurança – o único órgão que pode autorizar o uso excepcional da força (art. 42 da Carta⁵⁵⁹) – e o poder de obstaculizar o uso da força através do veto (art. 27(3)⁵⁶⁰), inclusive em relação a eles próprios. Em última análise, essas potências estão sujeitas a um regime de segurança diverso em relação ao restante dos Estados. Nessas condições, a consequência de uma proibição genérica à utilização da força a todos os Estados membros da ONU combinada com poderes de impedir sua utilização excepcional, conferidos aos Estados que compõem o núcleo permanente do Conselho significou, para estes, uma resultante positiva de poder.⁵⁶¹

⁵⁵⁸ Diz o texto do art. 2(4) da Carta da ONU: “Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas”.

⁵⁵⁹ Art. 42, Carta da ONU: “No caso de o Conselho de Segurança considerar que as medidas previstas no Artigo 41 seriam ou demonstraram que são inadequadas, poderá levar a efeito, por meio de forças aéreas, navais ou terrestres, a ação que julgar necessária para manter ou restabelecer a paz e a segurança internacionais. Tal ação poderá compreender demonstrações, bloqueios e outras operações, por parte das forças aéreas, navais ou terrestres dos Membros das Nações Unidas”.

⁵⁶⁰ Art. 27 (3), Carta da ONU: “As decisões do Conselho de Segurança, em todos os outros assuntos [não processuais], serão tomadas pelo voto afirmativo de nove membros, inclusive os votos afirmativos de todos os membros permanentes, ficando estabelecido que, nas decisões previstas no Capítulo VI e no parágrafo 3 do Artigo 52, aquele que for parte em uma controvérsia se absterá de votar”.

⁵⁶¹ Morgenthau argumenta que o poder do veto vicia a própria lógica do sistema de segurança coletiva que é o de assegurar que os propósitos agressivos de um Estado sejam freados pela combinação da força dos demais, ainda que estes não sejam diretamente atingidos. A prerrogativa de obstaculizar a utilização coletiva da força nesse sentido, ao isentar os membros permanentes do Conselho de Segurança dos próprios mecanismos que garantem a segurança internacional, bem assim dos países que com eles estão alinhados, contraria a essência do sistema. Cf.

Além disso, o contexto geopolítico do momento fez com que a proibição genérica de utilização da força favorecesse o equilíbrio de poder. Ascendendo como as duas principais potências militares após a Segunda Guerra Mundial, Estados Unidos e União Soviética bipolarizaram a distribuição global do poder e encontraram na prerrogativa do veto um meio de contenção recíproca.⁵⁶² Portanto a analogia entre a limitação da espionagem e a limitação da força não seria adequada a princípio, a não ser que se vislumbresse um mecanismo de compensação aos Estados com maior capacidade de inteligência que, guardadas as devidas proporções, fosse tão vantajoso quanto o poder do veto o é.

Pode-se dizer ainda que eventuais limitações à capacidade de inteligência dos Estados afetaria negativamente o dilema da segurança ao agravar a incerteza entre os Estados. Se um Estado tem reduzida sua capacidade de coletar informações sobre intenções de rivais e inimigos sua insegurança aumenta, motivando-o a obter mais poder para contrabalancear a incerteza. Dessa forma, a espionagem age como um *fator mitigador do dilema da segurança* ao reduzir o nível de incerteza entre os Estados, o que será melhor explorado na seção 6.2.

Reconhecendo em linhas semelhantes os mesmos problemas que ora se discutem, Ashley Deeks argumenta que as revelações de Edward Snowden alteraram a forma como os fatores que desacreditam eventuais propostas regulatórias são percebidos, provocando o que chamou de uma “mudança no agnosticismo com o Direito Internacional” em relação às possibilidades de regulação da vigilância^{563 564} – conceito que no texto da autora corresponde ao que aqui se denomina de espionagem de informações privadas.

MORGENTHAU, H. J. **Politics among...** *op. cit.* p. 232-242. Nessas condições, se o sistema de segurança coletiva operar em qualquer nível que não seja o ideal, ele terá o efeito oposto ao que almeja, o que Morgenthau denomina de “supremo paradoxo da segurança coletiva”. *Ibidem.* p. 333-334. Em crítica consonante, Ernest Gross questiona a própria ideia da delegação do poder a um Conselho centralizado em um sistema desenvolvido para funcionar segundo a lógica do equilíbrio de poder: “An assumption that a workable security system requires delegation of strategic power to a centralized structure condemns it to ineffectiveness from the outset. This is all the more true if the assumption extends to vesting in the system a preponderance, or balance, of power. Voluntary delegation of command authority – except to meet exigencies of an on-going war – has rarely, if ever, been found either practicable or acceptable”. GROSS, Ernest A. *International Organization and Collective Security: Changing Values and Priorities. Collected Courses of the Hague Academy of International Law*, 1973. p. 431.

⁵⁶² O alto número de vetos a que recorreram os dois países no período da Guerra Fria se comparados com o momento posterior evidencia essa relação. Cf. UNITED NATIONS. **Security Council Veto List**. Disponível em: <<http://research.un.org/en/docs/sc/quick>>

⁵⁶³ DEEKS, A. *An International Legal...* *op. cit.* p. 313-319.

⁵⁶⁴ Outros autores também manifestam otimismo em relação às possibilidades regulatórias, como por exemplo: KHALIL, Chantal. *Thinking Intelligently about Intelligence: a model global framework*

De acordo com a comentarista, os documentos vazados por Snowden evidenciam práticas de coleta de informações não relacionadas diretamente com a defesa da segurança nacional, o que aumentaria a necessidade de balizamento das atividades das agências. Paralelamente, argumenta que há um maior entendimento sobre as regras domésticas que disciplinam atividades de espionagem externa o que facilitaria o desenvolvimento de normas internacionais que estivessem alinhadas com a legislação interna, com isso aumentando as chances de cumprimento dos acordos que as previssem. Além disso, observa que as agências tem evidenciado um desejo “menos saliente” de manter o sigilo sobre suas capacidades de vigilância. Por fim, observa que os Estados que possuem maior capacidade de inteligência são aqueles que foram os mais atingidos pelas revelações, e por consequência, são os que sofrem a maior pressão política por adoção de normas que limitem suas atividades.⁵⁶⁵ Tudo levando a autora a concluir que, seja qual for o paradigma das relações internacionais de que se valha para aferir a possibilidade de criação de um parâmetro de regulação internacional das atividades de vigilância (realismo, institucionalismo, liberalismo e construtivismo) esse resultado provavelmente ocorrerá positivamente, ou os Estados irão considerar, normativamente, tal objetivo.⁵⁶⁶

Particularmente em relação ao realismo político, sustenta a autora que a ausência de regulação internacional da vigilância prejudicaria a formação ou manutenção de acordos de compartilhamento de informações entre Estados, reduzindo assim seu poder relativo. Isso ocorreria na medida em que a ausência da regulação poderia justificar o impedimento ou interrupção do compartilhamento por parte de um dos Estados por suspeitas de que a prática de coleta de um aliado afrontaria o Direito Internacional. Exemplificativamente, o judiciário canadense poderia determinar que o país interrompesse o compartilhamento de informações

protecting privacy. **The George Washington International Law Review**, v. 47, 2015; GENDRON, Angela. Just war, just intelligence: an ethical framework for foreign espionage. **International Journal of Intelligence and CounterIntelligence**, v. 18, n. 3, 2005; DANIELSON, Mark E. A. Economic Espionage: a framework for a workable solution. **Minnesota Journal of Law, Science & Technology**, v. 10, 2008; LEIGH, Ian. Democratic Control of security and Intelligence Services: a legal framework. In: **Security Sector Reform: Institutions, Society and Good Governance**, Geneva, 2003.

⁵⁶⁵ *Ibidem*. p. 315-319.

⁵⁶⁶ “[...] I consider here in broad terms why, regardless of the IR perspective(s) one adopts or of one’s view about what motivates states to act on the international plane, one should conclude that international regulation is likely to happen as a positive matter, or at least that states should consider regulation as a normative matter”. *Ibidem*. p. 323.

com os Estados Unidos porque, segundo seu entendimento, as práticas de coleta de informações da NSA seriam incompatíveis com o Direito Internacional, o que reduziria o poder dos dois países em termos de segurança. Ao contrário, ao adotar normas que regulassem a vigilância externa, afirma a autora, os países ocidentais ganhariam tanto em reputação quanto em eficiência em relação a Estados como Rússia e China. Seriam esses os argumentos que levam Ashley Deeks a afirmar que, mesmo sob a ótica realista, deve-se esperar uma “mudança no regime jurídico internacional” relativo à coleta de informações privadas.⁵⁶⁷

Antes de analisar os argumentos da autora é preciso considerar que as possibilidades regulatórias da espionagem internacional oscilam entre suas diferentes modalidades. Se foi demonstrado anteriormente na tese que há uma gradação no nível de tolerância entre as três modalidades de espionagem analisadas (seção 4.6), por consequência lógica é razoável supor que aquela espécie de espionagem a que corresponde o menor nível de tolerância – que é a espionagem de informações privadas – reflete maiores possibilidades de regulamentação. Mas não pelas razões apresentadas por Ashley Deeks.

De fato, os argumentos da autora não convencem. A princípio, as razões que apresenta para justificar uma mudança de percepção sobre as possibilidades regulatórias da espionagem internacional encerram uma concepção equivocada sobre o impacto das revelações de Snowden. O que se viu após as revelações foi, ao contrário do que sustenta a autora, uma preocupação maior das autoridades públicas dos Estados Unidos e Reino Unido com o sigilo das informações classificadas, a que correspondeu maior rigor com procedimentos de segurança da informação.

Além disso, a pressão política que exerce a sociedade civil sobre os governos destes países no que diz respeito aos seus serviços de inteligência é principalmente relacionada à proteção de sua privacidade enquanto cidadãos, de forma que a

⁵⁶⁷ “Some states, concerned that U.S. and UK foreign surveillance may violate international law, may feel obligated (or be ordered by their courts) to limit their current intelligence-sharing relationship with those states. To the extent that a lack of agreed surveillance norms reduces intelligence cooperation, this diminishes the power of states that otherwise would share intelligence. Adopting agreed surveillance norms could facilitate intelligence-sharing among norm-adhering states, allowing them to better protect themselves against threats by unfriendly states. [...] Instead, adopting such norms could give Western states both reputational and efficiency advantages over states such as Russia and China. And to the extent that realists view international law as a mirror of power relations among states, states such as the United States, United Kingdom, Germany, and several other European states remain powerful at this moment in time. Realists thus might expect a shift in the international legal regime to reflect the interests of those states”. Ibidem. p. 324.

coleta de informações de titularidade de governos, grupos e indivíduos estrangeiros é encarada como necessária à preservação da segurança nacional. Com efeito, do ponto de vista político, a narrativa de emergência de promoção da segurança nacional perante a ameaça terrorista, como discutido no capítulo 2, criou um ambiente favorável à potencialização dos serviços de inteligência de forma que propostas de regulação da atividade, especialmente quando direcionada a alvos externos, são frequentemente denunciadas como um aumento do risco à segurança nacional. Posto que tenha crescido a pressão interna da sociedade civil por maior rigor na proteção da privacidade, a mesma preocupação não se repete com relação às informações de governos, grupos e indivíduos estrangeiros, dado o importante papel que a retórica da segurança exerce politicamente em uma sociedade. Nessas condições, há suporte político interno para a condução de espionagem externa não-regulamentada por regras de Direito Internacional.

Não bastasse, os resultados que a autora extrai de uma leitura realista sobre o problema não parecem corretos. Em primeiro lugar porque a tolerância jurídica e política de determinada atividade significa maior liberdade de atuação do que a que haveria caso fosse ela juridicamente regulada. Ausência de regras ou uma regulamentação superficial, fragmentada ou deficiente é algo que favorece a condução da atividade, pois permite que o Estado que a realiza o faça sem restrições jurídicas quanto ao modo e à oportunidade em que deseje fazê-lo. Logo, parece óbvio concluir que, considerando as premissas realistas, grandes potências irão preferir conduzir a espionagem em um ambiente de liberalidade, que signifique possibilidades mais amplas de coleta de informação e, por consequência, potencialmente mais segurança.

É realmente possível, como sugere Ashley Deeks, que a criação de regras que disciplinem a prática da espionagem de informações privadas afaste preocupações internas que porventura existam em determinado Estado a respeito da ilicitude internacional de operações de coleta de informações recebidas de aliados, o que fomentaria a estabilidade de redes de compartilhamento. Não obstante, disso não decorre a conclusão de que haveria no caso um ganho em segurança para os Estados que compõem a rede como sugere a autora. Isso porque, a contribuição que uma empreitada de compartilhamento de inteligência oferece para a segurança dos Estados envolvidos não é determinada apenas pela *quantidade* de informações compartilhadas e pela estabilidade da rede, mas

principalmente pela *qualidade* das informações coletadas, isto é, a relevância que seu conteúdo tem para questões de segurança nacional. Dessa forma, é forçoso concluir que uma rede de compartilhamento que opere na ausência de regulação, ainda que eventualmente tenha que suportar a deserção de algum membro que decida não mais receber informações que foram obtidas por violação ao Direito Internacional⁵⁶⁸, irá aproveitar maior liberdade e terá maiores chances de obter as informações que realmente guardam algum valor para a segurança estatal. Em termos mais simples, a tolerância da espionagem internacional contribui para a *eficiência* de redes de compartilhamento de informações.

A verdade é que, como foi discutido na seção 4.3, o Direito Internacional já é dotado de regras e um arcabouço jurisprudencial suficientes para que se permita aferir as circunstâncias em que a espionagem de informações privadas possa ser considerada ilícita, contrária à proteção internacional do direito humano à privacidade. Por essa razão é que se identifica um baixo grau de tolerância jurídica relativo à espécie. O que se pode esperar em relação a eventuais mudanças no regime normativo nesse particular é, no máximo, uma reafirmação da proteção ao direito à privacidade no ambiente cibernético, como sinalizam decisões judiciais e resoluções da ONU, bem como maior clareza e precisão quanto às circunstâncias em que a espionagem de informações privadas “extra-jurisdição” violariam o Direito Internacional. Mais que isso seria um erro esperar, ao menos sob a ótica realista, considerando as razões de segurança anteriormente discutidas.

Por sua vez, a espionagem de segredos de empresa pode ter finalidades não-econômicas quando, por exemplo, é direcionada à obtenção de tecnologias militares de indústrias do setor terceirizado de defesa (*Lockheed Martin, Boeing etc.*). Nesse caso, valem as mesmas considerações sobre as dificuldades de se regular a espionagem de segredos de Estado. Diversamente, quando a espionagem de segredos de empresa é relacionada a estratégias de competitividade no comércio internacional, a princípio sua eventual regulação não acarretaria prejuízos à promoção da segurança. Não obstante, a dimensão econômica também é um

⁵⁶⁸ No caso dos Estados Unidos, ainda que alguns de seus aliados em redes de compartilhamento de informações possa encontrar alguma resistência interna quanto à licitude das operações, poucos são aqueles que podem se dar ao luxo de recusar o suporte da robusta capacidade de inteligência da NSA como complemento aos seus aparatos de segurança.

componente do poder nacional na ótica realista clássica⁵⁶⁹, de sorte que o ajuste de um compromisso constitutivo em relação à espionagem de segredos de empresa poderia influenciar relações de poder entre os Estados. Isso ocorreria na medida em que a quantidade e qualidade de segredos obtidos clandestinamente pelo Estado coletor fossem suficientes para se converter efetivamente em uma vantagem competitiva no mercado internacional em relação ao Estado de cujas empresas as informações foram coletadas. Em outros termos, uma alteração na relação de competitividade entre dois Estados repercutiria proporcionalmente em uma alteração na relação de poder econômico relativo entre eles. Se o Estado “A” obtém segredos de empresas do Estado “B” que lhe proporcionem em relação a este alguma vantagem competitiva no comércio internacional, pode-se dizer que “A” ganhou poder econômico em relação a “B”.

Partindo dessa premissa, seria possível sugerir que o Estado que suporte maior prejuízo em termos de competitividade, resultante da obtenção clandestina dos segredos de suas empresas, seria favorável ao ajuste de um compromisso internacional que limitasse ou proibísse a prática da espionagem econômica. Já o Estado agressivo em práticas de aquisição ilícita de tecnologias se posicionaria contrário ao estabelecimento de parâmetros regulatórios, preferindo realizar a atividade no ambiente de tolerância que atualmente define a espionagem econômica internacional.

Ocorre que essa relação não se estrutura de forma tão simples, numa lógica “Estado espião-Estado vítima”. No caso de China e Estados Unidos, como descrito na Introdução e no capítulo 3, a prática da espionagem econômica cibernética flui em uma “via de mão dupla” entre os dois países.⁵⁷⁰ Particularmente em relação à China, sua estratégia de aquisição de segredos de empresa via espaço cibernético pode ser compreendida no contexto da política de intervenção estatal no desenvolvimento tecnológico e científico de médio-longo prazo (*National Medium and Long-Term Plan for Science and Technology Development, 2006–2020*). Um dos objetivos centrais do plano consiste em “fomentar inovação original através de

⁵⁶⁹ Posto que os autores realistas clássicos analisem o aspecto econômico do poder como um “suporte” às capacidades militares, sem qualquer relação com a competitividade no comércio internacional. Nesse sentido, Morgenthau inclui os “recursos naturais” e a “capacidade industrial” como elementos do poder nacional. Cf. MORGENTHAU, H. **Politics...** *op. cit.* p. 82-88. Também associando o poder econômico como propulsor das capacidades militares, CARR, E. H. *op. cit.* p. 113 e ss.

⁵⁷⁰ A mesma conclusão alcançada em LINDSAY, J. R. *et. al. op. cit.*, Introduction.

co-inovação e re-inovação baseada em assimilação de tecnologias importadas” em cujas entrelinhas alguns comentaristas identificam disposição para obtenção ilícita de segredos de empresa “em uma escala nunca vista no mundo”.⁵⁷¹

Seria de se esperar então que a China considerasse favorável um ambiente de fracas proteções normativas internacionais a sistemas de segurança da informação. Entretanto, o ambiente de tolerância normativa com intrusões cibernéticas que favorece o desenvolvimento de sua política tecnológica e econômica poderá lhe afetar negativamente em outras esferas, especialmente militar. Nesse contexto, há um reconhecimento da superioridade do rival Estados Unidos para condução de operações ofensivas militares no espaço cibernético, justificando a preocupação com a segurança de seus sistemas.

De fato, o país tem coordenado algumas importantes iniciativas no âmbito da ONU no sentido de estabelecer parâmetros de responsabilidade estatal no que diz respeito à segurança da informação. Uma delas é a elaboração do *Código internacional de conduta para segurança da informação*, apresentado, juntamente com Rússia, Tajiquistão e Uzbequistão, na Assembleia Geral em 2011. O propósito do documento é “identificar os direitos e responsabilidades dos Estados no espaço informacional” assegurando que “tecnologias de informação e comunicação [...] sejam usadas exclusivamente para beneficiar o desenvolvimento econômico e social e o bem estar do povo, com o objetivo de manter a estabilidade e a segurança internacional”.⁵⁷²

Dentre os parâmetros de conduta sugeridos, destacam-se o compromisso de não utilizar tecnologias da informação para a prática de atos de agressão, ameaças

⁵⁷¹ Cf. LINDSAY, J. R.; CHEUNG, T. M. From Exploitation to Innovation: Acquisition, Absorption, and Application. In: LINDSAY, J. R. et. al. op. cit., p. 57 e MCGREGOR, James. **China's Drive for 'Indigenous Innovation'**: A Web of Industrial Policies. U.S. Chamber of Commerce, Global Intellectual Property Center, 2010. p. 4.

⁵⁷² “The purpose of the present code is to identify the rights and responsibilities of States in information space, promote their constructive and responsible behaviours and enhance their cooperation in addressing the common threats and challenges in information space, so as to ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and people's well-being, with the objective of maintaining international stability and security”. UNITED NATIONS GENERAL ASSEMBLY. **Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General**, A/66/359, Disponível em: <https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf>

à paz e segurança internacionais, e a proliferação de armas cibernéticas⁵⁷³; e de proteger o espaço cibernético e a infraestrutura crítica pertinente de ameaças, distúrbios, ataques e atos de sabotagem.⁵⁷⁴ Na versão atualizada do documento (2015), um dos enunciados denuncia a preocupação do eixo sino-russo em prevenir que “outros Estados” (leia-se Estados Unidos) explorem sua “posição dominante” sobre os recursos, infraestrutura, redes e tecnologias de informação e comunicação e produtos e serviços, o que poderia minar o “controle independente” dos Estados sobre esses fatores, ou ameaçar sua segurança política, econômica e social.⁵⁷⁵ Não há no documento menção expressa à obtenção clandestina de segredos de empresa ou a qualquer outra atividade que o valha.

É preciso reconhecer, fiel à inspiração realista que se aceita, que a abordagem *soft law* que vem sendo conferida ao problema dificilmente terá qualquer efeito na conduta dos Estados. Não obstante, ainda que precários os parâmetros propostos através desses instrumentos, denunciam eles a posição oficial de um Estado que os endossa diante das várias alternativas disponíveis para enfrentar um problema – inclusive a de não se adotar formalmente nenhum tipo de modelo de conduta. Por essa razão, é possível extrair algumas conclusões sobre a posição da China.

Analisando o teor do documento pode-se afirmar que um ambiente de completa liberdade de atuação no espaço cibernético, se favorece a China na condução da espionagem econômica, a prejudica em outras dimensões, principalmente militar e social – esta última que pode ser ameaçada por interferências externas que perturbem o forte controle estatal que se opõe à *internet* no país. Além disso, a posição dominante dos Estados Unidos e aliados ocidentais

⁵⁷³ “c) Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies”. *Ibidem*.

⁵⁷⁴ “(e) To reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage”. *Ibidem*.

⁵⁷⁵ “(5) To endeavour to ensure the supply chain security of information and communications technology goods and services, in order to prevent other States from exploiting their dominant position in information and communications technologies, including dominance in resources, critical infrastructures, core technologies, information and communications technology goods and services and information and communications networks to undermine States’ right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security”. UNITED NATIONS GENERAL ASSEMBLY. **Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General**, A/69/723, Disponível em: <<https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>>

sobre as tecnologias e infraestruturas de informação e comunicação motiva a China a pressionar por parâmetros regulatórios de conduta no espaço cibernético, mesmo que isso possa refletir em alguma constrição normativa às suas próprias atividades de espionagem. Em uma concepção realista, pode-se arriscar a dizer que a China percebe o problema sobre uma concepção relativa de poder: o resultado de eventual regulação da conduta dos Estados no espaço cibernético lhe favoreceria em maior medida do que lhe desfavoreceria, representando, portanto, uma resultante positiva de poder.

A tendência regulatória que parece surgir em relação à espionagem econômica é, portanto, de grau moderado, através de enunciados de reduzido valor normativo (códigos de conduta, resoluções etc.) e devida muito mais ao fato de ser necessário disciplinar as ações dos Estados no espaço cibernético do que propriamente a uma legítima disposição a se limitar a coleta de segredos de empresa através de compromissos internacionais.

5.2.3 *Dificuldades de fiscalização*

A espionagem, por definição, é uma atividade cuja execução se pretende ocorrer sem detecção. Um eventual acordo internacional que limitasse ou proibisse a prática da espionagem teria que prever mecanismos de fiscalização de seu cumprimento, o que poderia ser feito de duas maneiras.

Um método possível seria através do trabalho de órgãos internacionais de fiscalização – através de uma agência especializada da ONU, por exemplo – a que seria garantido acesso às agências nacionais de inteligência. Seria algo semelhante às inspeções da Agência Internacional de Energia Atômica. Haveria dois problemas com esse método, um de ordem técnica e outro atinente à segurança.

A princípio, haveria dificuldades em dotar esse órgão fiscalizador com expertise necessária para detectar eventual violação ao acordo, algo que não se verifica em qualquer organização internacional atualmente. Para ser eficaz, tal órgão precisaria ser capaz de atestar a ocorrência de intrusões cibernéticas ou operações de HUMINT quando denunciadas por algum Estado, inspecionar cabos submarinos de fibra ótica por onde trafegam dados de *internet* e, principalmente, ter algum nível de acesso às agências de inteligência.

Mesmo que essas dificuldades técnicas sejam superadas – pois em tese é possível que sejam – seria necessária ainda a convergência de um alto nível de confiança dos Estados no órgão fiscalizador, que deveria ser capaz de zelar pelo sigilo das informações e operações que porventura tome conhecimento durante suas atividades de inspeção. Do ponto de vista do Estado que aceita tal espécie de fiscalização isso representaria um grave comprometimento da segurança de suas informações, notadamente se considerarmos que o suposto órgão envolveria o trabalho de representantes de diversos Estados, inclusive inimigos. Os benefícios em se aceitar um tal tipo de ingerência deveriam compensar, em termos de cálculo relativo de ganho de poder, os riscos que a fiscalização representa para a segurança das informações do Estado inspecionado. Isso remete novamente à questão da limitação à segurança analisada na seção anterior: não há incentivos suficientes para que Estados com grande capacidade de inteligência se sujeitem a regimes de limitação ou inspeção de suas atividades de coleta de informação.

De outra forma que não a inspeção internacional, uma supervisão recíproca de um tal acordo pelos seus próprios membros somente seria eficaz através da própria espionagem, levando novamente a outro problema cíclico. Não havendo outra forma efetiva de supervisão de um acordo de tal natureza, os Estados se veriam pouco motivados a se vincular. Esse problema foi abordado por Rapahel Bitton nos seguintes termos:

Do ponto de vista de cada Estado, desistir de coletar informação significa praticamente aceitar uma espécie de cegueira nacional. De fato, essa cegueira iria cobrir as informações sobre o não-cumprimento de outros Estados com a regra contrária à espionagem porque esses outros Estados iriam presumivelmente conduzir sua espionagem clandestinamente. Esse é um ponto crucial pois a estabilidade de qualquer norma internacional depende da expectativa de cada nação de que as outras nações irão observá-la.⁵⁷⁶

Não bastasse, se para Estados e empresas a identificação de que suas informações foram coletadas é em muitos casos possível graças aos altos investimentos que fazem em sistemas de segurança da informação, o mesmo não

⁵⁷⁶ “From each state’s point of view, giving up intelligence-gathering means practically accepting a kind of national blindness. In fact, this blindness would extend to information about other states’ non-compliance with the rule against espionage because other states would presumably conduct their espionage clandestinely. This is a crucial point because the stability of any international norm hinges on each nation’s expectation that the other nations will observe it”. BITTON, R. op. cit. p. 1015.

ocorre com os indivíduos, de sorte que a fiscalização de um eventual tratado de limitação expressa da coleta de informações privadas de particulares incluiria complexidades peculiares às que foram anteriormente apresentadas. O alto número de alvos das operações – milhões de pessoas que não tem condições de identificar se tiveram suas informações privadas coletadas por alguma agência de inteligência – deixaria o ônus de fiscalização totalmente a cargo dos Estados ou de órgãos internacionais. Isso sem mencionar as complexidades técnicas inerentes a um processo de tal dimensão.

Em suma, nota-se que as dificuldades de monitoração de um acordo internacional de limitação à espionagem fazem com que sua eventual violação se revele um fácil ardil, desmotivando qualquer expectativa de eficácia do compromisso.

5.3 Conclusões provisórias: é necessário romper com ambiente de tolerância?

Uma leitura realista das possibilidades de se evoluir os parâmetros regulatórios aplicáveis às atividades de espionagem internacional nos mostra que avanços, em termos de criação de normas, são possíveis mas improváveis de ocorrer. O alto valor que os Estados atribuem à segurança interna e defesa nacional desmotiva a sujeição à constrições ao exercício da espionagem. Mesmo que haja uma tendência mais favorável à criação de limites mais rigorosos, em maior ou menor medida, para a coleta de informações privadas de particulares e segredos de empresa, a eficácia de eventual acordo que formalize tal limitação estaria seriamente comprometida por dificuldades de fiscalização.

É verdade que essas considerações se apoiam sobre a condição de que há a necessidade de manifestação do consentimento estatal para que novas obrigações de Direito Internacional vinculem um Estado. E, de fato, o argumento de que essa é mesmo a única forma de se obrigar um Estado sob normas de Direito Internacional é tradicional na doutrina.⁵⁷⁷ No entanto, admite-se hoje com maior tranquilidade que é

⁵⁷⁷ Louis Henkin, por exemplo, sustentou que: “*States make law by consent, by agreement. Inter-State law is made, or recognized, or accepted, by the "will" of States. Nothing becomes law for the international system from any other source*”. HENKIN, Louis. *International Law: Politics, Values and Functions. Collected Courses of the Hague Academy of International Law*, 1989. p. 46. No mesmo sentido, Prosper Weil quando afirma que: “*Absent voluntarism, international law would no longer be performing its functions*”. WEIL, P. *Towards Relative Normativity in International Law? The American Journal of International Law*, v. 77, 1983. p. 420. Vale ainda conferir a

possível que obrigações de Direito Internacional nasçam independentemente da vontade dos Estados⁵⁷⁸, sendo o exemplo mais claro dessa situação o surgimento de uma norma *jus cogens*.⁵⁷⁹

É realmente difícil vislumbrar qualquer cenário em que uma norma pertinente ao problema da espionagem internacional, em qualquer das suas modalidades, alcance algum tipo de consenso apto a alçá-las à categoria de Direito Internacional Geral, ou que ocorra o desenvolvimento de um padrão de comportamento estatal suficientemente coeso para solidificar um costume internacional. Mesmo que se admita por hipótese e para fins de argumentação que isso venha a ocorrer, o fato de nascer às margens do consentimento estatal poderia, de um lado, suplantar a resistência dos Estados diante de eventuais limitações à sua segurança, mas, por outro, as chances de observância a normas de tal natureza seriam ainda mais remotas. Certamente, seriam encaradas pelos Estados como afrontas à sua soberania.

É verdade que, na maior parte das situações, as normas de Direito Internacional são estritamente cumpridas pelos Estados, mesmo quando não há mecanismos sancionatórios e executórios correspondentes à sua eventual violação. Todavia, tratando-se de normas que afetam relações de poder relativo, serão elas violadas por Estados que se consideram prejudicados caso venham a cumprir suas obrigações. Como explica Morgenthau:

característica ênfase no princípio do consentimento que deu a tônica à escola soviética de Direito Internacional. Por todos, cf. TUNKIN, Grigorii Ivanovich. **Theory of international law**. Harvard University Press, 1974.

⁵⁷⁸ Para uma discussão ampla, conferir: TOMUSCHAT, Christian. Obligations arising for States without or against their will. **Collected Courses of the Hague Academy of International Law**, 1993.

⁵⁷⁹ O art. 53 da Convenção de Viena sobre o Direito dos Tratados, 1969, determina que: “É nulo um tratado que, no momento de sua conclusão, conflite com uma norma imperativa de Direito Internacional geral. Para os fins da presente Convenção, uma norma imperativa de Direito Internacional geral é uma norma aceita e reconhecida pela comunidade internacional dos Estados como um todo, como norma da qual nenhuma derrogação é permitida e que só pode ser modificada por norma ulterior de Direito Internacional geral da mesma natureza”. O caráter imperativo desse tipo de norma decorre exatamente da possibilidade de sua vinculação independentemente do consentimento dos Estados. De fato, aceitando-se que as normas *jus cogens* possuem formação costumeira, para que se reconheça seu caráter imperativo deve-se aceitar por consequência que mesmo a *objeção persistente* de um Estado não é apta a afastar sua obrigatoriedade, tal como ocorreria com uma norma costumeira “ordinária”. Um estudo sintetizado sobre as principais questões que envolvem o conceito e as implicações das normas *jus cogens* pode ser lido em: NASSER, Salem Hikmat. *Jus Cogens*: ainda esse desconhecido. **Revista Direito GV**, v. 1, n. 2, 2005.

A grande maioria de regras de Direito Internacional geralmente não são afetadas pela fragilidade do sistema de execução pois o cumprimento voluntário evita que o problema da execução se manifeste integralmente. O problema da execução se torna relevante, no entanto, naquela minoria de casos importantes e, no geral, espetaculares [...] nos quais a conformidade com o Direito Internacional e sua execução tem uma influência direta sobre o poder relativo das nações interessadas. Nesses casos, como nós temos visto, considerações de poder e não jurídicas é que determinam o cumprimento e a execução.⁵⁸⁰

É preciso reconhecer, como observa Andrew Guzman, que “questões de segurança são aberrativas em razão do enorme valor que Estados atribuem a problemas de segurança e sobrevivência nacional”.⁵⁸¹ Isso nos alerta a não reduzir o Direito Internacional a relações de poder, pois, de fato, Estados cooperam e respeitam as normas internacionais em diversas oportunidades em que interesses de reciprocidade estão envolvidos. Os realistas não ignoram isso, mas consideram que as relações que afetam o equilíbrio de poder são o que há de relevante na análise e na prática da política internacional, sendo periféricas as demais. Assim, pode-se dizer que o realismo explica “poucas e grandes coisas importantes”.⁵⁸²

Vale frisar ainda, para evitar qualquer confusão, que não se argumenta que eventuais regras convencionais de Direito Internacional não teriam eficácia sobre o comportamento dos Estados. Se esse fosse o argumento aqui desenvolvido, não faria sentido analisar os fatores que dificultam a regulação, pois seria ela mesmo inócua e seria irrelevante se um Estado contraísse ou não determinada obrigação pertinente ao exercício da inteligência, pois ele fatalmente não iria observá-la. Pelo contrário, o que se argumentou neste capítulo foi que existem particularidades na atividade da espionagem que, combinadas com peculiaridades do Direito

⁵⁸⁰ “Thus the great majority of rules of international law are generally unaffected by weakness of its system of enforcement from arising altogether. The problem of enforcement becomes acute, however, in that minority of important and generally spectacular cases, particularly important in the context of our discussion, in which compliance with international law and its enforcement have a direct bearing upon relative power of the nations concerned. In those cases, as we have seen, considerations of power rather than of law determine compliance and enforcement”. MORGENTHAU, H. **Politics**... *op. cit.* p. 230.

⁵⁸¹ “security issues are aberrational because of the enormously high value states place on issues of national security and national survival”. GUZMAN, Andrew T. **How International Law Works: a rational choice theory**. Oxford University Press, 2008. p. 72.

⁵⁸² Os dizeres são de Kenneth Waltz, mas atribuídos ao realismo estrutural em particular: “Structures never tell us all that we want to know. Instead they tell us a small number of big and important things. They focus our attention on those components and forces that usually continue for long periods”. WALTZ, K. N. Reflections on Theory of International Politics: a response to my critics. In: KEOHANE, R. O. [org.] **Neorealism and its Critics**. Columbia University Press, 1986. p. 329.

Internacional, obstaculizam um nível maior de regulação do que o que atualmente se verifica. Em suma, **o ambiente de tolerância irá prevalecer.**

Mas, se sob a ótica realista, as chances de se atingir um nível de regulação superior para a espionagem internacional são parcas, isso significa que o *status quo* da atividade – isto é, a atual configuração da distribuição dos poderes de coleta e segurança de informações sigilosas entre os Estados – é algo impassível de alteração? As normas de Direito Internacional proveriam o único caminho possível ou legítimo para mitigar os problemas relacionados ao exercício da espionagem em um ambiente de tolerância? Tratados e outras normas de Direito Internacional seriam as únicas ferramentas capazes de conter o poderio de inteligência das grandes potências, reduzindo o hiato que as separam de Estados menos aptos ao exercício da atividade? Um sonoro “Não!” se ouve dos autores realistas.

De fato, a ênfase do realismo político nas deficiências do Direito Internacional nos conduz a pensar em mecanismos de mudança social que não envolvam criação de regras constritivas mas que sejam capazes de interferir nos fatores reais de poder da sociedade internacional. Como alerta E. H. Carr, não se deve exagerar o papel da legislação pois “as mudanças mais importantes na estrutura da sociedade e no equilíbrio de forças que nela agem são realizadas sem ação legislativa”.⁵⁸³ Portanto, mais frutífero que pensar em formas de alteração na normativa internacional para equacionar os problemas atinentes à espionagem é refletir sobre o significado da escassez de normas – a tolerância – e maneiras de se alterar o *status quo* que não exijam criação de regras de limitação. Em outros termos, como **realizar mudanças sem ser necessário romper o ambiente de tolerância.** A estas tarefas se dedicará o capítulo seguinte.

Como a modalidade de espionagem de segredos de Estado é aquela associada ao mais alto grau de tolerância, sendo ainda a mais intimamente ligada às relações de poder e segurança entre Estados, é ela suficiente para delimitar a análise, razão pela qual se afasta da reflexão seguinte a espionagem de segredos de empresa e informações privadas de particulares.

⁵⁸³ “Even to-day, it is easy to exaggerate the role of legislation; and it may still be true to say (as it would certainly have been true a hundred years ago) that the most important changes in the structure of society and in the balance of forces within it are effected without legislative action”. CARR, E. H. *op. cit.* p. 212.

6 EFEITOS DO AMBIENTE DE TOLERÂNCIA DA ESPIONAGEM INTERNACIONAL DE SEGREDOS DE ESTADO E MECANISMOS DE INTERFERÊNCIA

“Oh yes, I know of you. I read your reports”.

(Nikita Khrushchev, líder soviético, ao ser apresentado ao Diretor de Inteligência Central dos Estados Unidos Allen Dulles, em um jantar na Casa Branca em 15 de setembro de 1959).⁵⁸⁴

Num cenário utópico ideal, as políticas e os métodos de governança dos Estados seriam absolutamente transparentes, sujeitos à crítica e fiscalização dos seus cidadãos e da comunidade internacional. Não haveria segredos e, por consequência, espionagem. Serviços de inteligência atuariam apenas para organizar e disseminar apropriadamente a informação coletada, toda ela publicamente disponível. Não haveria razões para desconfiança entre os Estados pois todos saberiam tudo sobre todos e, por consequência, a percepção de insegurança seria drasticamente aliviada. Nesse mundo ideal a balança do “saber” e do “segredo” penderia toda para o primeiro lado.

Esse cenário, como toda utopia, está muito distante da realidade. Tal como ocorre com a configuração heterogênea do poder econômico e bélico nas relações internacionais, os Estados possuem diferentes níveis de capacidade de obter e de proteger segredos. As agências de inteligência estatais contam com tecnologias, expertise e capacidades orçamentárias significativamente desiguais e isso naturalmente se reflete, juntamente com o poderio militar, político e econômico, na resultante de poder do Estado.

Nesse ambiente de desequilíbrio, o Direito Internacional pouco faz – pois pouco pode fazer nesse particular – para limitar o ímpeto de grandes potências da inteligência – impulsionado pela retórica da segurança na era do medo – pela coleta de segredos de outros Estados e assim reduzir, ao menos um pouco, a distância que as separa de Estados que contam com capacidades modestas ou quase nulas. Daí surge a caracterização de tolerância jurídica da espionagem internacional. Mas o que significa para as relações internacionais um ambiente de tolerância? Quais são

⁵⁸⁴ Como relatado em LATHROP, C. *op. cit.* p. 50.

as consequências práticas de um cenário não regulamentado sobre a espionagem internacional de segredos de Estado?

6.1 A tolerância da espionagem internacional como artifício de conservação do *status quo*

Uma primeira consequência que se nota é que a tolerância da espionagem internacional assume uma função de conservação da desigualdade em termos de exercício da inteligência entre grandes potências e Estados menos aptos à prática da atividade. É óbvio que as capacidades de conduzir a inteligência são principalmente determinadas por investimentos internos que os Estados fazem em seus aparatos de coleta e análise de informação. Assim, um Estado cujas capacidades de inteligência são modestas e que aumente os gastos com a atividade tende a reduzir o diferencial de poder que o separa de um Estado mais competente para a realização da tarefa. Mas o exercício da espionagem internacional, que em um ambiente de tolerância é praticamente irrestrito em termos jurídicos, poderia ser limitado caso houvesse regras que disciplinassem seu exercício – algo improvável de ocorrer, como visto. Naturalmente, mesmo nessa situação hipotética, as distintas capacidades de condução da inteligência continuariam a determinar um cenário de heterogeneidade em termos de poder de inteligência dos Estados. O papel que as regras teriam, nesse caso, seria o de limitar ou atenuar a disparidade que separa grandes potências da inteligência dos demais Estados e, principalmente, disciplinar, ainda que superficialmente, o exercício da atividade.

Uma das proposições centrais da teoria de Morgenthau, como foi visto (seção 5.1.2), é a de que o Direito Internacional exerce uma função ideológica de conservação do *status quo*, como uma força estática que contribui para determinada configuração de poder.⁵⁸⁵ De fato, em tantas dimensões em que a desigualdade de poderes é verificada (militar, econômica, comercial *etc.*), o mais comum é que o *status quo* seja preservado não pela tolerância, mas sim pelas próprias regras de Direito Internacional que disciplinam as relações entre os Estados em cada uma dessas áreas. Assim é que, a título de comparação, o poder de veto previsto na Carta da ONU permite a preservação da superioridade dos membros permanentes

⁵⁸⁵ MORGENTHAU, H. *Politics...* *op. cit.* p. 64.

do conselho de segurança em termos de utilização da força, compensando o regime de restrição geral (como discutido na seção 5.2.2). Da mesma forma, as políticas econômicas e comerciais hoje sugeridas (alguns diriam “impostas”) por países desenvolvidos aos países em desenvolvimento, através de instituições como OMC, Fundo Monetário Internacional – FMI, Banco Mundial, Organização para Cooperação Econômica e Desenvolvimento – OCDE, refletem a exigência de conformidade com padrões que em última análise favorecem a posição dos Estados mais ricos e dificultam o desenvolvimento dos demais.⁵⁸⁶ Como exemplo, o ajuste de normas de liberalização do comércio internacional e a criação da OMC foram acompanhadas da instituição de um regime comum de parâmetros mínimos de proteção à propriedade intelectual, favorecendo uma posição de vantagem dos Estados exportadores de tecnologia.

Mas se considerarmos que a ausência de regras é também uma manifestação do Direito, algo como um “silêncio eloquente” dos Estados que optam por não criar regras quando e onde poderia haver, podemos concluir que a tolerância da espionagem internacional é também um artifício do qual se valem as grandes potências para conservação do *status quo*, entendida como a atual configuração da distribuição do poder de inteligência entre os Estados. Isso se revela ainda mais persuasivo se considerarmos as proposições da abordagem *Lotus* (seção 4.5.1) para concluir que a tolerância é uma opção tácita pela permissividade do exercício da espionagem de segredos de Estado, de forma que a própria realidade, isto é, a disparidade de capacidades de inteligência, é o suficiente para conservar a posição favorável das grandes potências.

Uma vez que a tolerância da espionagem internacional contribui para a manutenção do *status quo* das grandes potências em termos de capacidade de inteligência, ela acaba por refletir positivamente em sua resultante de poder, pois conseguem elas obter segredos econômicos, políticos e militares, bem como proteger suas próprias informações perante a inteligência de outros Estados, de forma mais eficiente que os demais. Portanto, a tolerância da espionagem

⁵⁸⁶ No estudo *Kicking Away the Ladder*, o autor Ha-Joon Chang argumenta que os Estados desenvolvidos atualmente recomendam aos países em desenvolvimento políticas que eles mesmos não observaram quando estavam em estágio de desenvolvimento. Ao “esconderem o segredo do sucesso”, o que os países desenvolvidos acabam por promover, sustenta o autor, são dificuldades ao desenvolvimento dos demais. CHANG, Ha-Joon. **Kicking Away the Ladder: Development Strategy in Historical Perspective**. Anthem Press, 2002.

internacional favorece a preservação do *status quo* como um todo, não apenas no que diz respeito à configuração dos poderes de inteligência entre os Estados.

Sobre as proposições elaboradas, duas observações merecem ser feitas: em primeiro lugar, a relação que se estabelece entre capacidade de inteligência e preservação do *status quo* é válida até o ponto em que se aceite a premissa anteriormente estabelecida que define que a obtenção de informação significa acréscimo de poder ao Estado. Caso se afaste tal premissa, a validade da proposição fica condicionada a uma análise empírica que evidencie uma relação causal entre a obtenção de determinada informação e o aumento de poder.

Em segundo lugar vale ressaltar a constatação de que os Estados percebem o valor da atividade de inteligência de maneiras sensivelmente distintas. Enquanto há Estados que orientam a tomada de decisão e a política externa com forte apoio na inteligência, outros não almejam – ou não podem, por razões práticas, ter – influência significativa nas relações internacionais, atribuindo pouca ou nenhuma importância à inteligência externa. Dada sua “marginalidade”, esses últimos Estados são raramente alvos de operações de inteligência e em regra não percebem a desigualdade de poderes e a conservação do *status quo* como algo que lhes prejudique além do que a própria condição de inferioridade já o faça.

Mas em relação àqueles Estados que, apesar de menos eficazes na condução da atividade, realizam inteligência como suporte às suas políticas externa e doméstica e que buscam assumir posições estratégicas no cenário internacional, a conservação do *status quo* das grandes potências da inteligência é prejudicial segundo seu ponto de vista, como a maioria das manifestações de desigualdade. Enquanto potências da inteligência se valem de sua distinta capacidade de coleta e análise de informações para explorar uma posição de vantagem ligada ao *saber* sobre os outros e ao *segredo* sobre si mesmo, aqueles se veem significativamente limitados em fazer um ou outro. Dessa forma, os Estados de menor capacidade de inteligência apenas se conformam com o ambiente de tolerância da espionagem pois estão cientes dos mesmos obstáculos à regulação que foram discutidos no capítulo anterior. Sabem, portanto, que qualquer empenho em direção à regulação seria vão.

A partir dessa constatação, vale investigar se a tolerância produz alguma outra consequência, paralelamente ao efeito prejudicial de conservação do *status quo*.

6.2 A tolerância da espionagem internacional de segredos de Estado como atenuante do nível de incerteza no dilema da segurança

Uma das teorizações centrais do realismo político é a proposição do dilema da segurança de John Herz, que, como discutido anteriormente (seção 5.1.3), enfatiza a trágica situação de incerteza e desconfiança que confere a tônica das relações internacionais em um ambiente anárquico. Confrontados com o imperativo de sobrevivência e incapazes de saber com absoluta certeza quais as intenções dos rivais, os Estados tendem a suspeitar uns dos outros, o que provoca um ciclo vicioso de acumulação de poder para suplantarmos a insegurança gerada. Essa relação demonstra que um acréscimo de poder por parte de um Estado não implica necessariamente um ganho para sua segurança, pois, ao fazê-lo, ele motiva o acréscimo de poder de rivais, prejudicando, por consequência, sua própria segurança. De outra forma, um decréscimo de poder pode amenizar o sentimento de insegurança dos rivais mas agrava sua insegurança na medida em que não se pode saber com certeza se a outra parte nutre propósitos defensivos ou agressivos. Na incerteza e insegurança residiriam, portanto, a inescapável tragédia das relações internacionais.

É importante ressaltar, no entanto, que a proposição do dilema da segurança não conduz necessariamente à conclusão de que os Estados inseridos no dilema fatalmente serão levados ao conflito ou mesmo que todos os conflitos que ocorrem são provocados pelo dilema. O que é inevitável na formulação teórica é apenas a consequência de que a incerteza conduz à acumulação de poder pelos Estados. Mas isso não significa que o resultado da acumulação de poder será sempre o conflito porque os Estados podem *reduzir* o nível de incerteza até atingir a percepção de que o outro acumula poder para fins defensivos. Como explica Robert Jervis:

Um estado que pensa que o outro sabe que ele quer apenas preservar seu *status quo* e que seu armamento se destina apenas à auto-preservação irá concluir que o outro lado irá reagir ao seu armamento através do aumento de sua própria capacidade apenas se for agressivo ele próprio. Na medida em que o outro lado não é ameaçado, não há razão legítima para este último Estado objetar o

armamento do primeiro; dessa forma, a objeção provaria que o outro é agressivo.⁵⁸⁷

Note-se que essa condição só é válida até o limite em que se reconhece que é possível apenas reduzir o nível de incerteza, mas nunca eliminá-lo, pois, do contrário, haveria uma contradição lógica insuperável na proposição. Com efeito, aceitar que a incerteza pode ser eliminada seria o equivalente a afirmar que não há dilema algum, contrariando a premissa central da proposição. Logo, os Estados podem mitigar a incerteza ao sinalizar para outros que seu acúmulo de poder possui propósitos defensivos e, ao mesmo tempo, buscar se certificar de que o acúmulo de poder dos demais também atende apenas à mesma finalidade.

Mas como nunca se pode ter a absoluta certeza de que outros Estados não dissimulam suas reais intenções ou, mesmo acreditando em sua boa-fé, não se possa assegurar que futuramente o propósito defensivo inicial do acúmulo de poder não se converterá em um objetivo agressivo – o mesmo valendo para o próprio Estado, pois a alternância de governo pode interferir nos objetivos de sua política externa – o máximo que se pode fazer é tentar atenuar a incerteza. Dessa forma, o conflito provavelmente ocorrerá quando o nível de incerteza for grande o suficiente para provocar uma percepção não tolerável de insegurança. **Isso nos leva a concluir que o problema do dilema da segurança é uma questão de intensidade do nível de incerteza entre os Estados;** o dilema é inescapável mas pode ser gerido a fim de mitigar os efeitos deletérios da incerteza. Portanto, a cooperação é possível mesmo no dilema e será tão profícua quanto for a capacidade dos Estados em administrar o nível de incerteza entre eles.

O sucesso dessa administração, que objetiva reduzir a dúvida e a desconfiança, depende de um binômio: a) da capacidade do Estado de comunicar corretamente aos demais suas intenções pacíficas, puramente defensivas e b) da capacidade do Estado de compreender corretamente a intenção dos demais. Para cumprir a primeira tarefa o Estado pode sinalizar seus propósitos defensivos aos demais com ajustes em sua política militar, através de tratados de controle de

⁵⁸⁷ “A state which thinks that the other knows that it wants only to preserve the status quo and that its arms are meant only for self-preservation will conclude that the other side will react to its arms by increasing its own capability only if it is aggressive itself. Since the other side is not menaced, there is no legitimate reason for it to object to the first state's arms; therefore, objection proves that the other is aggressive”. JERVIS, Robert. Cooperation under the Security Dilemma, **World Politics**, v. 30, n. 2, 1978. p. 181.

armamentos ou de restrições unilaterais às suas capacidades bélicas.⁵⁸⁸ Um bom exemplo disso é a política de “não-primeiro uso” (*no first-use policy*) manifestada por algumas potências nucleares – mais enfaticamente pela China – com o objetivo de comunicar a finalidade exclusivamente defensiva/retaliatória de seu arsenal atômico.⁵⁸⁹

Obviamente, como um Estado avalia relações de poder de forma relativa, ele apenas irá adotar políticas constritivas de poder se acreditar que um outro Estado rival também o fará, o que depende do sucesso da segunda tarefa, isto é, de saber precisamente quais são as verdadeiras intenções dos demais Estados. E o meio mais eficaz para fazê-lo é a espionagem. Ao possibilitar a coleta dos segredos mais sensíveis de um Estado, a espionagem permitirá aferir se as ambições de outra parte são, de fato, puramente defensivas. Pois um Estado que esteja formalmente comprometido com um acordo de controle de armamento ou alguma outra forma de limitação de empoderamento pode nutrir intenções contrárias e ocultar atividades que violariam os termos do ajuste. Nesse contexto, a contração de obrigações constritivas em um acordo internacional pode servir ao propósito de tranquilizar a incerteza de rivais, aliviar pressões e desviar atenções, enquanto nos bastidores se faz exatamente o oposto daquilo que se diz fazer.

Nesse sentido, a espionagem serve como um corretivo a um nível “profundo” de segredos de Estado que atinge informações que não poderiam escapar ao conhecimento da comunidade internacional dada sua extrema sensibilidade para assuntos de segurança. O desenvolvimento de armas de destruição em massa seria um bom exemplo desse tipo de informação. Em razão de seu grave risco para a segurança dos Estados, a confidencialidade de informações pertinentes ao desenvolvimento e à posse desse tipo de armamento agrava o dilema da segurança e a instabilidade internacional. Como não há norma de Direito Internacional capaz de impedir que um Estado mantenha sob segredo informações de tal natureza, ou qualquer outro tipo de informação – a menos que tenha o Estado voluntariamente se obrigado à sua divulgação por tratado – deve-se recorrer à espionagem de segredos de Estado como única forma eficaz de mitigar um nível perigoso de confidencialidade. Em outros termos, **para equilibrar os efeitos nocivos que um**

⁵⁸⁸ GLASER, Charles L. Realists as Optimists: Cooperation as Self-Help. *International Security*, v. 19, n. 3, 1995. p. 68-69.

⁵⁸⁹ Cf. YU, Rong; GUANGQIAN, Peng. Nuclear No-First-Use Revisited. *China Security*, v. 5, n. 1, 2009.

nível forte de tolerância de se manter segredos possa provocar no dilema da segurança, deve-se admitir por reflexo também um nível forte de tolerância da espionagem internacional. Dessa forma, ao contribuir para a redução do nível de incerteza e, por consequência, insegurança entre os Estados, a tolerância da espionagem internacional de segredos de Estado, em última análise, favorece a estabilidade internacional.

Não obstante, três variáveis interferem nessa relação. A primeira delas diz respeito à desigualdade de poderes de inteligência entre os Estados. Com efeito, é forçoso reconhecer que a tolerância da espionagem internacional irá favorecer aqueles Estados que possuem capacidades de inteligência mais avançadas, por serem eles mais eficientes em obter e ocultar segredos. Dessa forma, Estados com grandes capacidades de inteligência estão mais aptos a reduzir sua incerteza sobre os demais e ao mesmo tempo optar se querem ou não reduzir o nível de incerteza dos demais sobre si mesmos. Isso ocorre na medida em que eles podem decidir se comunicam de boa-fé informações que denunciem seu propósito defensivo a outro Estado ou se ocultam segredos que possam evidenciar um intuito agressivo, simulando intenções defensivas para enganar a outra parte. Por essa razão, o ambiente de tolerância da espionagem internacional mitiga de forma mais eficaz os efeitos indesejados da incerteza entre Estados que possuem capacidades análogas de inteligência, como ocorreu com Estados Unidos e União Soviética durante a guerra fria.⁵⁹⁰ Estados com capacidades modestas de inteligência continuarão a perceber o ambiente de tolerância como uma ameaça à sua esfera de confidencialidade que não conseguem compensar com um nível satisfatório de coleta de informações sobre outros Estados, agravando, portanto, sua posição estratégica na política internacional.

⁵⁹⁰ Um bom exemplo de como a espionagem contribuiu para estabilizar relações durante a guerra fria foi a descoberta da instalação dos mísseis soviéticos em Cuba. O conjunto de informações repassadas pelo Coronel Oleg Penkovsky, espião a serviço dos Estados Unidos posicionado na União Soviética, reforçadas por imagens aéreas obtidas através de sobrevoos de aviões U-2 sobre a ilha, muniram a Casa Branca com subsídios suficientes para confrontar o regime comunista, na medida em que demonstraram que a capacidade balística dos soviéticos era menor do que se imaginava. Isso permitiu antecipar negociações para a resolução de uma crise que poderia acumular complicadores o suficiente para não se poder alcançar desfecho que não fosse bélico. De fato, em negociações secretas mantidas entre o presidente J. F. Kennedy e Nikita Krushchev, foi estabelecido que a retirada dos mísseis de Cuba seria acompanhada da desativação de bases de lançamento norte-americanas na Turquia e na Itália, o que efetivamente ocorreu. Cf. BESCHLOSS, Michael. **Mayday, Eisenhower, Khrushchev and the U-2 Affair**. New York: Harper and Row, 1988.

A segunda variável que interfere na relação entre a tolerância da espionagem internacional e o nível de incerteza diz respeito à eficácia dos serviços de inteligência. É que, como discutido anteriormente (seção 1.2.4), as agências de inteligência são passíveis de erros ou porque ignoram determinadas informações ou interpretam de forma errônea aquelas que logrou coletar. Por essa razão, o ambiente de tolerância da espionagem somente favorece a redução das incertezas se os serviços de inteligência acertam em suas análises. Do contrário, a aferição equivocada das intenções dos Estados rivais ou conduzirá a uma “falsa insegurança” (falso positivo), agravando a instabilidade das relações, ou a uma “falsa segurança” (falso negativo), última hipótese que, ainda que possa reforçar a estabilidade das relações a princípio, no longo prazo irá resultar em mais insegurança quando identificado o erro.

Exemplos ilustrativos de “falso negativo” na comunidade de inteligência dos Estados Unidos, a que se recorre aqui a título exemplificativo, são vários: a crença de que a União Soviética não enviaria mísseis para Cuba em 1962⁵⁹¹; a incapacidade de antecipar a invasão da Coreia do Norte sobre o Sul em 1950⁵⁹², a revolução iraniana de 1979⁵⁹³, a invasão do Iraque sobre o Kuwait em 1991⁵⁹⁴ e os testes nucleares conduzidos pela Índia em 1998.⁵⁹⁵ Neste último caso, a notável habilidade da Índia em conduzir operações de engano possibilitaram o desenvolvimento de seu armamento nuclear à surpresa do ocidente. Os indianos sabiam com exatidão quando as câmeras do satélite norte-americano teriam por alvo o local de testes e assim puderam sincronizar aparatos de camuflagem para tais momentos. Além disso, aumentaram a atividade em outros locais de teste para desviar a atenção da inteligência dos Estados Unidos. No plano político, a diplomacia indiana ofereceu garantias de que o país não ambicionava o desenvolvimento de armas nucleares.⁵⁹⁶

⁵⁹¹ KNORR, Klaus. Failures in national intelligence estimates: the case of the Cuban missiles. **World Politics**, v. 16, n. 3, 1964.

⁵⁹² BETTS, Richard K. Surprise despite warning: Why sudden attacks succeed. **Political Science Quarterly**, v. 95, n. 4, 1980. p. 562.

⁵⁹³ JERVIS, Robert. **Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War**. Cornell University Press, 2010.

⁵⁹⁴ DIAMOND, John. **The CIA and the Culture of Failure: US Intelligence from the End of the Cold War to the Invasion of Iraq**. Stanford University Press, 2008. p. 107-108.

⁵⁹⁵ JOHNSON, L. K. **Handbook...** *op. cit.* p. 7.

⁵⁹⁶ *Ibidem.* p. 7.

A operação foi respondida pelo rival Paquistão com cinco outros testes nucleares simultâneos, o que foi acompanhado da aprovação de sanções econômicas pelo Conselho de Segurança da ONU aos dois países. Entre Índia e Paquistão a força da dissuasão nuclear foi o que evitou um conflito militar e o agravamento das tensões de ambos com Washington apenas foi integralmente revertida após os ataques de 11 de setembro de 2001 – no caso do Paquistão, dada a necessidade de se criar alianças estratégicas para a “guerra ao terror”; em relação à Índia, em razão do propósito de estabelecer um “contrapeso” à ascensão chinesa na Ásia.⁵⁹⁷

Já o caso que melhor ilustra a situação do “falso positivo” é a falha da inteligência norte-americana ao atestar que o regime iraquiano de Saddam Hussein possuía armas de destruição em massa, como discutido na seção 1.2.4 (cf. também **Anexo 1**). A crença em uma circunstância inexistente justificou um conflito bélico absolutamente desnecessário baseado em reivindicações de prevenção, em uma clara expressão de como uma falha de inteligência interfere negativamente no dilema da segurança. É verdade que, em última análise, a decisão de invadir o Iraque já havia sido tomada na Casa Branca, de forma que a forte pressão política exercida sobre a comunidade de inteligência direcionou uma conclusão que serviu apenas para legitimar uma escolha já feita.⁵⁹⁸ Esse problema conduz à análise da terceira variável que interfere na relação entre a tolerância da espionagem e o nível de incerteza no dilema da segurança.

Pois, para que a tolerância da espionagem possibilite uma redução do nível de insegurança através da diminuição da incerteza é necessário que os líderes de Estado escolham políticas de não-agressão se a inteligência indicar que, da mesma forma, um rival adota uma posição pacífica exclusivamente defensiva. Contrariamente, caso as autoridades de um Estado guardem propósitos agressivos que não estão necessariamente relacionados à sua percepção de segurança, a indicação da inteligência de que um rival não apresenta ameaças irá apenas reforçar um estado de fragilidade do qual aquele se aproveitará.

Todas essas variáveis mostram que a tolerância da espionagem internacional de segredos de Estado apenas produz o efeito benéfico de redução da incerteza e,

⁵⁹⁷ KREPTON, Michael. Looking Back: The 1998 Indian and Pakistani Nuclear Tests. **Arms Control Today**, Arms Control Association, 11 jun. 2008.

⁵⁹⁸ Como já se argumentou na seção 1.2.5.

por consequência, da insegurança, caso sejam atendidas as três condições: i) entre Estados que possuam capacidades análogas de inteligência; ii) se a inteligência for correta em sua análise; iii) se os líderes de Estado forem fiéis a propósitos defensivos quando reduzida a incerteza.

Com efeito, todas essas condicionantes podem colocar sob questionamento a proposição de que a espionagem é a melhor forma para reduzir a incerteza entre os Estados. Assim, seria possível argumentar que uma outra possibilidade para atingir esse efeito seria se valer dos mecanismos formais de verificação previstos em tratados de controle de armamentos.

6.2.1 *Espionagem e mecanismos formais de verificação*

Há, de fato, uma diferença conceitual entre a espionagem e a verificação convencionada, na medida em que esta última pressupõe uma relação jurídica previamente estabelecida entre os Estados aos quais são conferidas prerrogativas de fiscalização, bem como possibilita a qualificação jurídica do comportamento fiscalizado – isto é, se violador ou não dos termos do acordo.⁵⁹⁹ O controle de armamentos ajustado entre Estados Unidos e União Soviética no *SALT I* e no *ABM Treaty*, ambos de 1972, estabelecia que: “cada parte pode usar de meios técnicos nacionais de verificação à sua disposição de maneira consistente com princípios de Direito Internacional reconhecidos em geral” e o compromisso de não interferir e não “utilizar de medidas deliberadas de dissimulação” diante dos meios técnicos nacionais de verificação da outra parte. Essencialmente, as mesmas prerrogativas e obrigações se repetem nos acordos de controle de armamentos que foram ajustados dali em diante.⁶⁰⁰

⁵⁹⁹ M. Fabien Lafouasse sustenta que são quatro os elementos que compõem a verificação: “Ces composantes sont successivement: l'existence d'une norme juridique de base, contenant les engagements qui sont l'objet de la vérification; l'acquisition des données de fait relatives au comportement des États soumis à l'obligation en cause; l'analyse des données précédemment recueillies; enfin, la qualification juridique des comportements observés. Seuls le recueil et l'analyse des données sont des phases communes à la vérification et à l'espionnage ; ce dernier, en effet, ne suppose aucune norme de base particulière entre Etat observateur et Etat observé, de sorte qu'en matière de désarmement l'espionnage et les méthodes d'intelligence contraires à la législation de l'État en cause sont prohibés, et au minimum inopposables à cet État”. LAFOUASSE, M. F. *op. cit.* p. 80.

⁶⁰⁰ WHEELER, Michael O. The Philosophical Underpinnings of Arms Control. In: WILLIAMS, Robert E. Jr.; VIOTTI, Paul R. [orgs.] **Arms Control: History, Theory and Policy**. Praeger Security International, v. 1, 2012. p. 69.

Em atenção a essas diferenças, seriam então os mecanismos de verificação um meio mais eficiente do que a espionagem para reduzir as incertezas entre os Estados e, assim, aliviar a percepção de insegurança? Em primeiro lugar vale observar que, especificamente em relação aos acordos mencionados, as duas partes nunca buscaram definir com precisão o que se deveria entender por “meios técnicos nacionais de verificação”.⁶⁰¹ Enquanto algumas hipóteses, como por exemplo, o envio de espiões, claramente não se enquadra no conceito de “meio técnico”, outras, como o reconhecimento por satélites, certamente consistia em uma de suas formas.⁶⁰² Mas em relação à maioria das outras formas de emprego dos meios de verificação é extremamente difícil definir se foge ou não ao escopo do acordo. Além disso, como fiscalizar a correição do emprego dos próprios mecanismos de verificação se não através da espionagem, sem incorrer em um problema cíclico?

Já o argumento de que os mecanismos formais de verificação estabelecem uma relação de confiança dada sua natureza convencional não é persuasivo. Isso porque, confiança e verificação são noções paradoxais. Estados que se vinculam a um compromisso de manutenção de propósitos defensivos ou redução de capacidades bélicas e ao mesmo tempo ajustam mecanismos paralelos de monitoração não confiam; na verdade desconfiam. Se há confiança não é necessário monitorar, fiscalizar, supervisionar; seria ela condição suficiente para afastar suspeitas quanto a eventuais dissimulações de intenções por parte de outros Estados. “*Trust but verify*”, a célebre frase proferida por Ronald Reagan logo após a assinatura do *Intermediate-Range Nuclear Forces (INF) Treaty*, em dezembro de 1987, não significa outra coisa que não “*Do not trust!*”.

Realmente, o **problema central da segurança nas relações internacionais não é aumentar o nível de confiança entre os Estados, mas sim reduzir o nível de incerteza**, que, como visto, são tarefas distintas. Como não há confiança de que Estados irão cumprir com determinado acordo de controle de armamento sem ser necessário prever mecanismos de verificação, não há também confiança a assegurar que um Estado não irá tentar trapacear fora da esfera de fiscalização. Em outras palavras, se não se pode confiar no cumprimento do acordo sem recorrer à

⁶⁰¹ *Ibidem.* p. 69.

⁶⁰² Como terminou por ser aceito tanto por Estados Unidos quanto União Soviética. Cf. WOLTER, D. *op. cit.* p. 31.

verificação, também não se pode confiar no respeito à própria verificação. Logo, se o que define então esse tipo de relação é a desconfiança e a incerteza, que se recorra então à espionagem como forma complementar de aferir as reais intenções de outro Estado.

É verdade que o nível e a extensão da verificação ajustada possam ser tão intrusivos que dificultem seriamente e desmotivem tentativas de trapaceas, ou mesmo que haja uma legítima intenção do Estado verificado em respeitar integralmente os termos do acordo. Mas antes de se cogitar essa hipótese é preciso ponderar se um Estado que se submete a um programa rígido de verificação o permite porque está comprometido com o acordo ou porque está seguro de que irá conseguir trapacear diante de suas restrições. Nesse sentido, a espionagem que seja dirigida complementarmente à verificação como forma de obter clandestinamente informações sensíveis de alto grau de sigilo resultará em redução das incertezas na medida em que, ou confirma as conclusões da verificação e o respeito de outro Estado ao acordo ou identifica eventuais trapaceas que escaparam à atenção da fiscalização. É preciso reconhecer ainda que não há nada que assegure que a espionagem será dirigida apenas à coleta de informações relacionadas ao cumprimento dos termos do acordo, mas o mesmo se pode dizer da verificação. Como observou Michael Wheeler,

é difícil vislumbrar como alguém iria provar que os meios técnicos nacionais [de verificação] estão sendo usados apenas para a monitoração do tratado e certamente não há garantias de que se um tratado for rompido em uma crise, a informação coletada pelos meios técnicos nacionais não serão usadas para outras finalidades.⁶⁰³

É razoável admitir, em atenção a esse problema, que a verificação conduzida por um órgão internacional permite um controle maior sobre a própria atividade de fiscalização e a utilização das informações para a estrita finalidade de aferição do cumprimento dos termos do acordo. Mas, por outro lado, a limitação dos órgãos internacionais de verificação para conduzir atividades clandestinas prejudica em alguma medida sua eficácia. Pois, por ser eminentemente técnica, ela somente extrai conclusões sobre as intenções do Estado verificado de forma indireta. Já a

⁶⁰³ “it is difficult to envision how one would prove that NTM is being used solely for treaty monitoring, and certainly there could be no assurances that if a treaty collapses in a crisis, the information gathered by NTM might not be put to other uses”. WHEELER, M. *op. cit.* p. 69.

espionagem tem o potencial de obter informações diretamente do alto escalão político do Estado monitorado e assim aferir com maior precisão suas verdadeiras intenções, sejam elas fiéis ou não ao acordo ajustado.

Um exemplo concreto que oferece particularidades interessantes para se refletir a relação da espionagem com a redução das incertezas e, paralelamente, os mecanismos formais de verificação, reside no recente acordo nuclear firmado entre Irã e os cinco membros permanentes do Conselho de Segurança da ONU mais a Alemanha (P5+1), o chamado *Joint Comprehensive Plan of Action (JCPOA)* (Viena, 2015).⁶⁰⁴

Através do ajuste, o Irã se compromete a limitar sua capacidade nuclear ao reduzir o número de suas centrífugas por 10 anos – para o máximo de 5.060, em oposição às mais de 20.000 que antes operava – e seu estoque de urânio por 15 anos – ao máximo de 300Kg – que não pode ser enriquecido além de 3,67%. Além disso, entre muitas outras restrições e compromissos técnicos, o país não poderá construir reatores de água-pesada adicionais ou acumular qualquer excesso do material por 15 anos. O cumprimento dessas e outras obrigações em matéria nuclear serão objeto de rígida monitoração por parte da Agência Internacional de Energia Atômica, inclusive sob possibilidade de inspeção *in loco*.

Em contrapartida, o Irã poderá explorar seu potencial atômico para fins energéticos e um conjunto de sanções econômicas impostas por Estados Unidos, União Europeia e ONU serão paulatinamente retiradas, permitindo a retomada da importação de petróleo do Irã – cuja suspensão acumulava perdas de aproximadamente 160 bilhões de dólares desde 2012 – e o acesso a cerca de 100 bilhões de dólares em ativos congelados no exterior.⁶⁰⁵

A opção do governo Barack Obama em firmar um acordo nuclear com o Irã sinaliza o reconhecimento de que os Estados Unidos não seriam capazes de impedir o rival de alcançar o desenvolvimento de armas atômicas apenas com embargos e sanções que dificultassem a aquisição dos equipamentos e materiais necessários à tanto. Para além disso, uma empreitada militar no país que objetivasse a destruição de sua capacidade nuclear seria ineficiente e catastrófica, pois envolveria outros

⁶⁰⁴ O texto integral do acordo pode ser lido em: UNITED STATES DEPARTMENT OF STATE. **Joint Comprehensive Plan of Action**, 2015. Disponível em: <<http://www.state.gov/documents/organization/245317.pdf>>

⁶⁰⁵ IRAN nuclear deal: Key details. **BBC News**, 16 jan. 2016. Disponível em: <<http://www.bbc.com/news/world-middle-east-33521655>>

atores (Israel, Rússia, Arábia Saudita entre outros) com possibilidade de escalada regional. Nesse cenário, Estados Unidos e aliados consideram como sendo a melhor opção um acordo que, ainda que temporário, permita saber se o Irã está mesmo comprometido com a utilização da energia nuclear para propósitos não bélicos.⁶⁰⁶

A responsabilidade dos Estados Unidos e aliados em assegurar que o acordo surtirá os efeitos desejados é extrema. Se nos anos que se seguirem ao término do ajuste o Irã vier a desenvolver armas nucleares, o acordo será considerado o elemento chave que possibilitou ao país realizar suas ambições de hegemonia regional e certamente Washington será culpado por um dos maiores erros políticos e estratégicos da história.

Nesse contexto, parece razoável supor que os Estados Unidos não confiariam a supervisão do acordo exclusivamente às inspeções da AIEA. A espionagem provavelmente irá assumir um papel complementar decisivo na identificação de eventuais desvios e mudanças de política que o regime iraniano porventura determine em relação ao cumprimento dos termos do tratado. De fato, um dos pontos centrais da argumentação favorável ao acordo nuclear quando se vê questionada sobre as limitações da inspeção técnica internacional é que:

[...] nenhum mecanismo de verificação é perfeito. No fim, boa inteligência é a ferramenta mais importante para detectar atividades secretas, mas inteligência e rígidas inspeções irão se complementar, tornando menos provável que o Irã assuma o risco de realizar atividades secretas e mais provável que os Estados Unidos as identifiquem se o Irã o tentar.⁶⁰⁷

Arrisca-se a afirmar que os Estados Unidos não celebrariam um acordo de tal natureza se não pudessem recorrer livremente à espionagem como instrumento complementar aos mecanismos de verificação internacional. Nesse sentido, pode-se dizer que a tolerância da espionagem internacional, significando liberdade de se recorrer a métodos clandestinos de coleta de informação sobre o futuro cumprimento do acordo nuclear, contribuiu para a estabilidade política das relações EUA-Irã.

⁶⁰⁶ Uma excelente sumarização dos principais compromissos firmados no acordo e dos argumentos a ele contrários e favoráveis pode ser lida em: SAMORE, Gary [org]. **Decoding the Iran Nuclear Deal**. Harvard Kennedy School, Belfer Center for Science and International Affairs, 2015.

⁶⁰⁷ “Of course, no verification measures are perfect. In the end, good intelligence is the most important tool for detecting secret activities, but intelligence and enhanced inspections will complement each other, making it less likely that Iran will take the risk of pursuing secret activities and more likely that the U.S. will catch Iran if it tries”. *Ibidem*. p. 38.

Apesar de não se poder ter uma exata dimensão das operações de inteligência dos Estados Unidos e aliados no Irã na atualidade, a ocorrência de um fato recente indica que os norte-americanos, de fato, não consideram suficiente os mecanismos formais de verificação. Em agosto de 2016 um membro do grupo iraniano de negociação do acordo nuclear foi preso sob acusações de envolvimento com a inteligência norte-americana e/ou britânica (os relatos são conflitantes neste ponto), sinalizando a condução de operações de HUMINT sobre o programa nuclear do país.⁶⁰⁸

6.3 Redes de compartilhamento de informações como mecanismo de interferência no ambiente de tolerância

A análise feita nas seções anteriores permitiu concluir que o ambiente de tolerância da espionagem internacional possibilita a redução das incertezas entre os Estados e, por consequência, sua insegurança, atendidas condições específicas. Concluiu-se também que esse efeito se realiza de forma mais eficaz entre Estados que possuem capacidades análogas de inteligência, sendo que, em situação de desigualdade, o ambiente de tolerância da espionagem serve à conservação do *status quo*.

Ocorre que, perante determinada configuração de poder, há Estados que estão satisfeitos e, portanto, adotam políticas de conservação do *status quo* e outros que, inconformados, buscam mudança. Nesse contexto, pode-se afirmar que a política do Estado com relação à sua inteligência externa acompanhará a política externa geral: se um Estado conduz políticas de aquisição de poder e alteração do *status quo* ou se, diversamente, se orienta por políticas de conservação de poder e preservação do *status quo*, a inteligência apoiará uma ou outra agenda.

É preciso observar antes de prosseguir na análise das políticas de preservação e alteração de *status quo* que a avaliação das relações de poder é uma tarefa complexa e sujeita a erros. Como alertou Morgenthau, por não existir um critério de avaliação absoluta da somatória do poder nacional, ela somente pode ser realizada de forma comparativa, ponderando-se o poder de um Estado relativamente

⁶⁰⁸ Cf. FITSANAKIS, Joseph. Conflicting details on Iranian nuclear negotiator arrested for espionage. **Intelnews.org**, 30 ago. 2016. Disponível em: <<https://intelnews.org/tag/iranian-nuclear-program/>> e BBCNEWS. **Iran arrests nuclear deal negotiator on spying charges**, 28 ago. 2016. Disponível em: <<http://www.bbc.com/news/world-middle-east-37209945>>

a outro. Assim, alterações relativas de poder devem ser pensadas como pesos em uma balança que são trocados de um prato para outro,⁶⁰⁹ de sorte que a avaliação correta de relações de ganho/perda ou superioridade/inferioridade de poder dependem tanto da correção da percepção que um Estado possui de seu próprio poder quanto do poder de outros Estados. Portanto, qualquer tentativa de avaliação feita por um observador externo será precária na medida em que não se pode identificar e quantificar todos os fatores que interferem nas relações de poder entre dois ou mais Estados.

Estabelecida tal ressalva e nos limites dessa possibilidade, sugere-se que, em termos de poder e políticas externas de inteligência, os Estados podem ser reunidos em quatro grupos:

1) Em primeiro lugar há os Estados Unidos e aliados estratégicos que colaboram em acordos permanentes ou circunstanciais de compartilhamento de informações (e.g.: Reino Unido, Canadá, Austrália, Nova Zelândia, Singapura, Coreia do Sul, Israel, e alguns países europeus). Esse grupo percebe o ambiente de tolerância da espionagem internacional como algo favorável, pois implica maior liberdade na coleta de informações e ao mesmo tempo determina um resultado de maior poder relativo perante Estados com menores capacidades de inteligência, seja porque ele próprio possui grande capacidade ou porque está aliado com um país que o tenha. Por perceberem que o ambiente de tolerância da espionagem favorece a estabilidade das relações com outras potências da inteligência rivais, os Estados que compõem esse grupo defendem a conservação do *status quo*, desde que mantenham sua superioridade relativa;

2) Em segundo lugar há Rússia e China que são Estados com grande capacidade de inteligência mas que conduzem políticas de aquisição de poder direcionadas à alteração do *status quo*. Os dois países são os únicos que demonstram atualmente políticas expansionistas que rivalizam a hegemonia norte-americana, de sorte que a supremacia dos Estados Unidos em termos de poderio de espionagem de segredos de Estado lhes é prejudicial. Portanto, o ambiente de

⁶⁰⁹ “The balance of power, mechanically conceived, is in need of an easily recognizable, quantitative criterion by which the relative power of a number of nations can be measured and compared. For it is only by means of such a criterion, comparable to the pounds and ounces of a real pair of scales, that one can say with any degree of assurance that a certain nation tends to become more powerful than another or that they tend to maintain a balance of power between them. Furthermore, it is only by means of such a criterion that variations in power can be converted into quantitative units to be transferred from one scale into the other in order to restore the balance”. MORGENTHAU, H. **Politics...** op. cit. p. 151.

tolerância da espionagem, apesar de poder lhes favorecer relativamente a Estados com baixas capacidades de inteligência, os prejudica comparativamente aos Estados Unidos;

3) Países que detêm pouca capacidade de inteligência mas que buscam uma maior inserção estratégica na política internacional (por exemplo, Brasil e África do Sul). Esses Estados se veem prejudicados pela tolerância da espionagem internacional em razão da desigualdade que os separa das potências da inteligência. Na medida em que almejam uma participação mais relevante nos assuntos internacionais, pretendem alterar o *status quo* em uma direção que os aproxime daqueles Estados;

4) Estados que se situam em uma posição marginal ao problema da tolerância da espionagem pois detêm capacidades baixas ou quase nulas de condução da espionagem externa ou guardam posições de isolamento ou neutralidade em que a atividade de inteligência não interfere.

Se a tolerância da espionagem internacional afeta Estados de formas diferentes, quais medidas devem eles adotar para reforçar um ou outro tipo de política. Em outros dizeres: o que se pode fazer para, de um lado, conduzir uma política de conservação do *status quo* que se beneficia da tolerância ou, de outro, uma política de alteração do *status quo* que, prejudicada pela tolerância, adota medidas que lhe acrescem o poder relativo sem, contudo, romper com o ambiente de ausência de regulação?

Do ponto de vista dos três primeiros grupos, uma medida comum que racionalmente deve ser adotada por todos Estados que os compõem é reforçar seus aparatos de segurança da informação. Tal medida é compatível tanto com a política de conservação quanto de alteração do *status quo* uma vez que limita o conhecimento de rivais sobre informações estratégicas que dizem respeito à condução da sua política externa, reforçando assim uma ou outra agenda. Isso pode ser feito através do reforço de protocolos de segurança, técnicas de contra-inteligência e, principalmente, adesão à criptografia e sistemas de proteção de redes.

Da mesma forma, potencializar sua capacidade de coleta de informações através do aumento de investimentos no serviço de inteligência é uma medida óbvia, mas que nem todos Estados são capazes de suportar. Enquanto os gastos que os Estados Unidos suportam com inteligência não encontra paralelo no mundo, outros

países dedicam parcelas ínfimas de seu orçamento ao serviço de inteligência. Tudo depende da força que a retórica da segurança exerce sobre a opinião pública e o parlamento de um país para que se consiga aprovar aumento de gastos com a inteligência.

Para além de medidas que interfiram na capacidade direta de inteligência, a reunião dos Estados em grupos conforme sugerido acima indica um potencial para a formação de alianças estratégicas, através de redes de compartilhamento de informações. A princípio, acordos de compartilhamento de informações são ajustados para potencializar e qualificar a coleta de informação. Como observa Ashley Deeks, uma agência de inteligência estrangeira pode contar com maior entendimento de aspectos culturais de problemas locais, como por exemplo Israel no Oriente Médio. Outros Estados adquiriram expertise no combate ao terrorismo, e podem fornecer informações valiosas para a condução de operações, a exemplo do Paquistão. Mesmo a posição geográfica de um Estado pode justificar seu valor em um acordo de compartilhamento dada a proximidade das fontes de informação.⁶¹⁰

Por serem secretos, é impossível analisar com precisão como e entre quais Estados esse tipo de acordo é ajustado. No entanto, sequentes vazamentos de informações classificadas permitiram algum conhecimento sobre a rede de compartilhamento *Five Eyes*, que tem seu germe na cooperação da inteligência dos Estados Unidos e Reino Unido na segunda guerra mundial e que posteriormente recebeu a adesão de outras democracias anglófonas: Canadá, Austrália e Nova Zelândia. Dedicada à inteligência de sinais, a rede tem acesso aos principais cabos submarinos por onde trafegam dados de *internet* (cf. seção 1.2.2, “b”). Segundo James Cox, cada parceiro coleta informação sobre uma área específica do globo de acordo com suas prioridades nacionais. Apesar de não se saber detalhes específicos sobre tais atribuições, há indícios de que a Austrália monitore o sul e o leste da Ásia; Nova Zelândia cubra o pacífico sul e o sudeste asiático; Reino Unido direcione sua atenção à Europa e ocidente da Rússia e os Estados Unidos monitore o caribe, a China, a Rússia, o Oriente Médio e a África.⁶¹¹

Além da rede *Five Eyes* os Estados Unidos mantêm outros acordos de compartilhamento de informações que vão se tornando mais restritos de acordo com

⁶¹⁰ DEEKS, Ashley. Intelligence Communities, Peer Constraints, and the Law. **Harvard National Security Journal**, v. 7, 2015. p. 7-8.

⁶¹¹ COX, James. **Canada and the Five Eyes Intelligence Community**. Canadian International Council, 2012. p. 6.

o número de membros: com Dinamarca, França, Holanda e Noruega (*nine eyes*); Alemanha, Bélgica, Itália, Espanha e Suécia (*fourteen eyes*).⁶¹² Outros acordos mais abrangentes aliam membros da OTAN na tarefa de compartilhamento de informações⁶¹³ e outros, mais restritos, Coreia do Sul e Singapura.⁶¹⁴

Essas alianças evidenciam bem a opção dos Estados que compõem o primeiro grupo. Do ponto de vista dos Estados Unidos, a cooperação com outros países aumenta a abrangência de suas operações, facilitando e potencializando a coleta de informações através de parceiros estratégicos. O seu protagonismo faz com que se tenha grande poder de influência para negociar os termos dos acordos, permitindo ajustar o nível do compartilhamento proporcionalmente à relevância da contribuição que faz outro Estado. Por fim, através da cooperação os Estados Unidos podem driblar as fortes restrições legais impostas por sua legislação doméstica à inteligência, se valendo de parâmetros mais frouxos adotados em outros países para receber informações que não poderia ele próprio coletar (o que ocorre particularmente na coleta de informações privadas, como discutido na seção 4.3.1). Já sob a ótica dos aliados, a cooperação com a robusta inteligência norte-americana permite suprir as deficiências de seus próprios serviços de inteligência com o recebimento de informações que eles não conseguiriam obter por si só. Além disso, alguns dos acordos de compartilhamento prevêem cláusulas de não espionagem entre os membros, favorecendo a posição de atores mais frágeis que, fora da rede, certamente seriam alvos da inteligência dos Estados Unidos.⁶¹⁵

Rússia e China – o segundo grupo – por sua vez, conduzem políticas de aquisição de poder e desafio à hegemonia norte-americana, do que é sintoma a expansão militar⁶¹⁶ e territorial sobre, respectivamente, a Crimeia e as ilhas do Mar

⁶¹² MACASKILL, Ewen; BALL, James. Portrait of the NSA: no detail too small in quest for total surveillance. **The Guardian**, 2 nov. 2013. Disponível em: <<https://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance>>; DENMARK is one of the NSA's '9-Eyes'. **Chp Post Online**, 4 nov. 2013. Disponível em: <<http://cphpost.dk/news/international/denmark-is-one-of-the-nas-9-eyes.html>>

⁶¹³ COX, J. *op. cit.* p. 7.

⁶¹⁴ DORLING, Philip. Singapore, South Korea revealed as Five Eyes spying partners. **The Sydney Morning Herald**, 25 nov. 2013. Disponível em: <<http://www.smh.com.au/technology/technology-news/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html>>

⁶¹⁵ COX, J. *op. cit.* p. 7 e DEEKS, A. Intelligence Communities... *op. cit.* p. 26.

⁶¹⁶ De 2006 a 2015 os gastos militares da Rússia cresceram de cerca de 47 Bilhões de dólares para aproximadamente 91 Bilhões, apesar de que em 2016 o orçamento militar foi reduzido em razão de fortes quedas no preço do petróleo. Já a China, no mesmo período, evoluiu de um patamar de 92 Bilhões de dólares em 2006 para 214 Bilhões em 2016. Os dois países representam respectivamente o quarto e segundo maiores gastos militares do mundo, sendo que o maior fica a cargo dos Estados Unidos, que em 2016 gastou 596 Bilhões de dólares e, em terceiro lugar,

do Sul da China. O fato de estar o rival comum na posição de “maestro” de uma rede de compartilhamento de informações de proporções globais faz com que a opção racional adequada à China e Rússia seja a criação de sua própria rede, aliando parceiros estratégicos como o Irã e a Índia, por exemplo. Nesse sentido, uma rede de compartilhamento de informações de países que adotam políticas de alteração do *status quo* exerceria um papel de contra-aliança às redes ocidentais, fortalecendo sua capacidade de coleta de segredos de Estado que favorecessem suas estratégias contra-hegemônicas. Além disso, a criação de um novo “polo global” de inteligência poderia servir de alternativa à alta dependência que a ONU tem da inteligência norte-americana, principalmente no que diz respeito às decisões do Conselho de Segurança de, por exemplo, aprovar ou não determinada sanção ou conduzir operações de paz.

Note-se que a aliança formada através de uma rede de compartilhamento de informações significa apenas cooperação em inteligência, não exigindo um alinhamento político externo mais abrangente. Ou seja, Estados que trocam informações não precisam necessariamente ser parceiros econômicos e muito menos aliados militares; basta que haja interesse em cooperar na tarefa de inteligência. Prova disso é o Paquistão, talvez o único verdadeiro aliado da China atualmente⁶¹⁷, e ao mesmo tempo um valioso parceiro dos Estados Unidos na cooperação em atividades de inteligência e combate ao terrorismo.

Por fim, o terceiro grupo, composto de Estados que possuem capacidades modestas de inteligência e que almejam uma participação mais relevante nos assuntos internacionais, tem como melhor opção se aliar ou ao primeiro ou ao segundo grupo. A criação de uma rede de compartilhamento entre eles próprios conduziria a uma cooperação pouco eficaz pois sua expertise em inteligência é deficiente e os recursos que dedicam à tarefa são escassos, de forma que seu não alinhamento com nenhum dos dois outros grupos significaria um isolamento perigoso

Arábia Saudita que, superando o orçamento russo, gastou 87 Bilhões em 2016. Cf. STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE. **SIPRI Military Expenditure Database**. Disponível em: <<https://www.sipri.org/databases/milex>>

⁶¹⁷ Trata-se da observação de Yan Xuetong a respeito da política externa chinesa. Em entrevista, ele observa o fato de que a China declarou publicamente em 2013 que não é uma aliada da Coreia do Norte e que as relações entre os dois países são piores do que entre China e Coreia do Sul, esta um aliado dos Estados Unidos. Resta então apenas o Paquistão como real aliado, especialmente diante da política de evitar alianças que o governo chinês tradicionalmente conduz nas últimas décadas. Cf. HUANG, Yufan. Q. and A.: Yan Xuetong Urges China to Adopt a More Assertive Foreign Policy. **The New York Times**, 9. fev. 2016. Disponível em: <http://www.nytimes.com/2016/02/10/world/asia/china-foreign-policy-yan-xuetong.html?_r=0>

em termos estratégicos. É verdade que estes Estados percebem o ambiente de tolerância como algo prejudicial, dada a desigualdade de capacidades de inteligência que os separam dos Estados dos dois outros grupos. Não obstante, na medida em que se aliem, seja com os Estados Unidos ou com o hipotético eixo Sino-Russo, o ambiente de tolerância não mais lhes seria desfavorável pois receberiam informações providas da espionagem que não conseguiriam de outra forma coletar, ao mesmo tempo em que iriam adquirir expertise ao longo do processo de cooperação.

Está claro que todas as asserções que foram feitas até aqui sobre as alianças em redes de compartilhamento de informações se silenciam sobre diversos detalhes que poderiam interferir nas consequências de cada forma de alinhamento. É possível que um acordo de compartilhamento especifique se a troca de informações será limitada a matérias específicas, como por exemplo combate ao terrorismo, tráfico internacional de armas ou entorpecentes ou mesmo proliferação nuclear. É possível também que o compartilhamento se restrinja a um tipo específico de inteligência (por exemplo, SIGINT) ou que não envolva a troca de segredos militares. Pode ocorrer também que um mesmo Estado compartilhe informações com dois outros que entre si são rivais, mas o faça em áreas diferentes como, por exemplo, segurança e assuntos econômicos. Outra possibilidade seria o ajuste de um acordo que prevesse para um Estado o recebimento de informações da inteligência de outro em troca de algo diverso de informações, que poderia ser auxílio financeiro, suporte técnico ou transferência de tecnologia, por exemplo. Todavia, todas estas variáveis foram isoladas para que fosse viável a elaboração do modelo, ainda que excessivamente abstrato, de formação de alianças estratégicas como um meio eficaz de se interferir no ambiente de tolerância da espionagem internacional.

Assim, sugere-se que as redes de compartilhamento, como um mecanismo que altera a configuração do equilíbrio de poder entre os Estados, servem tanto às políticas de conservação do *status quo* e preservação do ambiente de tolerância, quanto políticas de alteração do *status quo* independentemente da criação de regras de Direito Internacional que pudessem limitar o exercício da atividade.

7 CONCLUSÃO

Há algo de evasivo na espionagem que resiste ao conhecimento. O segredo que a define impõe um silêncio que aconselha o político a não dizer, o jurista a não agir e o acadêmico a não estudar. E assim os problemas associados à atividade se desintegram em discursos vazios, soluções efêmeras e análises precárias, de tal modo que a dificuldade em se lidar com o segredo convenientemente conduziu a espionagem a uma esfera de marginalidade de que a Política e o Direito Internacional não conseguem se apropriar integralmente. Dessa forma, a maneira contraditória de que políticos abordam o problema da espionagem e a escassez de regras de Direito Internacional que potencialmente a ele se aplicam estabelecem um ambiente de tolerância da atividade.

Mas a liberdade de que se vale um Estado para manter sigilo de suas próprias informações e operações de coleta de informação – em outras palavras, a prerrogativa do segredo – é aquela que autoriza outro Estado a fazer o mesmo. E nesse ponto é que uma força contrária ao segredo age: a pressão por saber, dirigida ao rompimento do segredo. Estados, portanto, se valem dessas duas forças segundo sua conveniência, de forma que ter segredos, espionar e ser espionado são consequências normais do ambiente de tolerância. Da incapacidade dos Estados de gerir a relação de antagonismo que se estabelece entre, de um lado o segredo e, de outro, a necessidade de saber, surgem os principais problemas relacionados à espionagem internacional, sejam eles de ordem jurídica ou política.

Entre o *saber* e o *segredo* há a incerteza; incerteza que gera insegurança; insegurança que gera medo. De fato, com o advento dos ataques terroristas de inspiração extremista islâmica ao mundo ocidental, Estados Unidos e aliados escolheram um inimigo comum e uma narrativa que sustentasse seu projeto de emergência, baseado na promoção da segurança. A percepção de que os ataques terroristas muitas vezes poderiam ter sido previamente identificados por atividades de inteligência e, por consequência, impedidos, foi o fator propulsor da expansão das capacidades dos serviços de inteligência ocidentais. Tais capacidades, como ficou evidenciado por sequentes vazamentos de documentos classificados, possibilitam a coleta de informações privadas de particulares em escala massiva,

segredos de valor econômico para obtenção de vantagens concorrenciais e segredos oficiais de Estados de importância estratégica militar e política.

Diante das revelações, cogitar a viabilidade do ajuste de um tratado internacional que disciplinasse atividades de espionagem entre os Estados foi uma reação imediata. De fato, juristas, em geral, são treinados para pensar e resolver problemas sociais em termos de criação de regras e por isso tendem a acreditar que regular é sempre o melhor caminho. Não obstante, uma leitura realista das causas que determinam a tolerância jurídica da espionagem que até o momento se verifica convence de que o resultado regulatório é extremamente improvável. O alto valor que os Estados atribuem à segurança interna e defesa nacional desmotiva a sujeição a constrições ao exercício da espionagem. Mesmo que haja uma tendência mais favorável à criação de limites mais rigorosos, em maior ou menor medida, para a coleta de informações privadas de particulares e segredos de empresa, a eficácia de eventual acordo que formalize tal limitação estaria seriamente comprometida por dificuldades de fiscalização. Portanto, o ambiente de tolerância provavelmente irá prevalecer.

Mas as normas de Direito Internacional proveriam o único caminho possível ou legítimo para mitigar os problemas relacionados ao exercício da espionagem em um ambiente de tolerância? Quais seriam exatamente as consequências de um ambiente desregulado para o exercício da espionagem? É verdade que, por possuírem capacidades distintas de inteligência, a tolerância afeta os Estados de forma diferente. Estados com maiores capacidades serão mais aptos a, ao mesmo tempo, proteger seus segredos e obter os segredos dos demais. Na medida em que o ambiente de tolerância favorece a perpetuação dessa desigualdade, as grandes potências se apoiam na carência de regras limitadoras para conservação desse *status quo*, entendido como a atual configuração da distribuição do poder de inteligência entre os Estados. Uma vez que a tolerância da espionagem internacional contribui para a preservação dessa condição, ela acaba por refletir positivamente na resultante de poder das grandes potências, pois conseguem elas obter segredos econômicos, políticos e militares de forma mais eficiente que os demais, o mesmo se podendo dizer de sua capacidade de proteger suas próprias informações perante a inteligência de outros Estados.

Diversamente, tratando-se de Estados que possuem capacidades análogas ou próximas de inteligência, a tolerância da espionagem produz um efeito benéfico

de atenuação do dilema da segurança. O permanente estado de incerteza que leva os Estados a acumular poder para propósitos defensivos mas que, ao fazê-lo, motiva o acúmulo de poder dos demais, pode ser reduzido através do conhecimento de informações que sinalizem a verdadeira intenção de rivais. Nesse sentido, a espionagem serviria como um corretivo a um nível “profundo” de segredos de Estado que atinge informações que não poderiam escapar ao conhecimento da comunidade internacional dada sua extrema sensibilidade para assuntos de segurança. Logo, para equilibrar os efeitos nocivos que um nível forte de tolerância de se manter segredos possa provocar no dilema da segurança, deve-se admitir, por reflexo, também um nível forte de tolerância da espionagem internacional. Ao contribuir para a redução do nível de incerteza e, por consequência, insegurança entre os Estados, a tolerância da espionagem internacional de segredos de Estado, em última análise, favorece a estabilidade internacional.

Por fim, sugere-se que, em um ambiente de tolerância da espionagem em que a mudança através de criação de regras é improvável, a melhor forma pela qual os Estados podem interferir no equilíbrio de poder é se reunindo em redes de compartilhamento de informações – cooperação que não necessariamente deve se refletir em alinhamentos militares. O que já fazem Estados Unidos, Reino Unido e outras democracias anglófonas pode ser repetido por Rússia e China como estratégia contra-hegemônica de alteração do *status quo*. Estados com menores capacidades de inteligência tem como opção se alinhar a um ou outro eixo na medida em que a criação de uma rede de compartilhamento entre eles próprios conduziria a uma cooperação pouco eficaz dada sua modesta expertise e carência de recursos. Além disso, seu não alinhamento com nenhum dos dois outros grupos significaria um isolamento perigoso em termos estratégicos.

Obviamente, todas as conclusões alcançadas valem enquanto se aceite as premissas teóricas sobre as quais a pesquisa foi conduzida. A adoção de uma abordagem crítica do Direito Internacional, enfática sobre a flutuabilidade de seus conceitos centrais e manipulabilidade da argumentação jurídica, favoreceu a caracterização do ambiente de tolerância como carência de uma resposta precisa que o Direito possa fornecer ao problema. A rejeição da abordagem crítica com a adoção de uma abordagem formalista não colocaria tanta ênfase na carência de regras expressas e argumentaria que o Direito Internacional oferece os mecanismos necessários para solucionar mesmo os casos difíceis.

Da mesma forma, a associação da atividade de inteligência com as relações de poder entre os Estados, a improbabilidade da regulação internacional da espionagem e as proposições do dilema da segurança somente se mostram coerentes caso se aceite as premissas do realismo político. Relações de poder não assumiriam um papel tão relevante caso se adotasse alguma teoria alternativa das Relações Internacionais que enfatizasse mecanismos de cooperação institucional ou questões de legitimidade, por exemplo. O problema é que nenhuma teoria das Relações Internacionais é absolutamente imune à crítica. Todas elas possuem pontos fortes e fracos de argumentação e, portanto, estão sujeitas à contra-argumentação recíproca.

Definitivamente este trabalho não encerra uma teoria nos estritos moldes consagrados pelo método de investigação científica, mas oferece as bases para a elaboração de uma. A classificação tridimensional da espionagem segundo a natureza da informação e do seu titular oferece um caminho seguro para pesquisas futuras sobre o assunto – que serão cada vez mais frequentes, ao que tudo indica. Além disso, reuniu-se na tese um número considerável de documentos, dados e referências a episódios ligados à espionagem internacional que podem facilitar outros trabalhos de investigação. Já a discussão sobre a licitude dos atos de espionagem contribui um pouco para suprir uma carência na literatura jurídica sobre o problema. Por fim, do ponto de vista das Relações Internacionais, o resgate do mais tradicional paradigma de análise para explicar o problema da espionagem no atual contexto político internacional acompanha a proposta de revisitação do realismo político clássico que ganhou força nos últimos anos.

REFERÊNCIAS

1. Literatura

ABBOTT, Kenneth W. *Modern International Relations Theory: A Prospectus for International Lawyers*. **Yale Journal of International Law**, 1989.

AID, Matthew. **The Secret Sentry**: the untold history of the national security agency. Bloomsbury Press, 2009.

ALEXY, Robert. **Constitucionalismo Discursivo**. Tradução: Luís Afonso Heck. 3 ed., 2011.

_____. **The Argument from Injustice**: A Reply to Legal Positivism. Tradução de Stanley L. Paulson e Bonnie Litschewski Paulson. Oxford University Press, 2002.

ANDREW, Christopher; MITHROKIN, Vasili. **The Sword and the Shield**: The Mitrokhin Archive and the Secret History of KGB. Basic Books, 1995.

BAHERI, Zahra; FARD, Ali Shojaei. Status of espionage from the perspective of international laws with emphasis on countries' diplomatic and consular relations. **Journal of Scientific Research and Development**, v. 2, n. 1, 2015.

BAKER, Christopher D. Tolerance of International Espionage: a Functional Approach. **American University International Law Review**, v. 19, n. 5, 2003.

BANKS, William C. Cyber Espionage, Surveillance, and International Law: Finding Common Ground. In: **Texas A&M Law Review Symposium**, 17 out. 2014. p. 6. Disponível em: <<http://ssrn.com/abstract=2558155>>

BAUMAN, Zygmunt; BIGO, Didier; ESTEVES, Paulo; GUILD, Elspeth; JABRI, Vivienne; LYON, David; WALKER, R. B. J. After Snowden: Rethinking the Impact of Surveillance. **International Political Sociology**, v. 8, 2014. p. 134.

BERGEN, Peter L.; ROTHENBERG, Daniel. **Drone Wars**: Transforming Conflict, Law and Policy. Cambridge University Press, 2015.

BERGIER, Jacques. **Secret Armies**: The Growth of Corporate and Industrial Espionage. Tradução de Harold J. Salemson, Indianapolis: Bobbs-Merrill, 1975.

BESCHLOSS, Michael. **Mayday, Eisenhower, Khrushchev and the U-2 Affair**. New York: Harper and Row, 1988.

BESSON, Samantha; TASIOULAS, John. **The Philosophy of International Law**, Oxford University Press, 2010.

BETTS, Richard K. Surprise despite warning: Why sudden attacks succeed. **Political Science Quarterly**, v. 95, n. 4, 1980.

BIERSTEKER, Thomas J.; SPIRO, Peter J.; SRIRAM, Chandra Lekha; RAFFO, Veronica. **International Law and International Relations**: Bridging theory and practice. Routledge, 2007.

BITTON, Raphael. The Legitimacy of Spying Among Nations. **American University International Law Review**, v. 29, n. 5, 2014. p. 1014-1015.

BORN, Hans; CAPARINI, Marina [orgs.]. **Democratic Control of Intelligence Services**. Ashgate, 2007.

BOUCHOUX, Deborah E. **Intellectual Property**: The Law of Trademarks, Copyrights, Patents and Trade Secrets. 4 ed., Delmar Cengage Learning, 2013.

BOWETT, D. W. **Self-Defence in International Law**. Manchester University Press, 1958.

BURCHILL, Scott; LINKLATER, Andrew; DEVETAK, Richard; DONNELLY, Jack; PATERSON, Matthew; REUS-SMIT, Christian; TRUE, Jacqui. **Theories of International Relations**, 3 ed., Palgrave Macmillan, 2005

BYMAN, Daniel. **Al Qaeda, the Islamic State, and the Global Jihadist Movement**: What Everyone Needs to Know. Oxford University Press, 2015.

CAMILLI, Edoardo. The Paris attacks. A case of intelligence failure? **NATO Review Magazine**, 2015. Disponível em: <<http://www.nato.int/DOCU/review/2015/ISIS/Paris-attacks-terrorism-intelligence-ISIS/EN/index.htm>>

CARLTON, David; SCHAERF, Carlo [org.] **The Dynamics of the Arms Race**. Croom Helm, 1975.

CARR, Edward Hallet. **The Twenty Years' Crisis 1919-1939**: an introduction to the study of international relations, 2 ed., Macmillan, 1946.

CEPIK, Marco Aurelio. Sistemas Nacionais de Inteligência: Origens, Lógica de Expansão e Configuração Atual. **DADOS – Revista de Ciências Sociais**, v. 46, n. 1, 2003.

_____; ANTUNES, Priscila. Brazil's New Intelligence System: An Institutional Assessment. **International Journal of Intelligence and Counterintelligence**, v. 16, 2003.

CHANG, Ha-Joon. **Kicking Away the Ladder**: Development Strategy in Historical Perspective. Anthem Press, 2002.

CHEN, Lung-Chu. **An Introduction to Contemporary International Law**: a policy-oriented perspective. Oxford University Press, 3 ed., 2015.

CHESTERMAN, Simon. The Spy Who Came in From the Cold War: Intelligence and International Law. **Michigan Journal of International Law**, v. 27, 2006.

CHURCHILL, Ward; WALL, Jim Vander. **The COINTELPRO Papers**: Documents from the FBI's Secret Wars Against Domestic Dissent. South End Press, 1990.

CLARK, Ransom J. **Intelligence and National Security**: A Reference Handbook. London: Praeger Security International, 2007.

COEN, Ross. **FU-GO**: The Curious History of Japan's Balloon Bomb Attack on America. University of Nebraska Press, 2014.

COHEN, Julie E. What Privacy is For. **Harvard Law Review**, v. 26, 2013.

COX, James. **Canada and the Five Eyes Intelligence Community**. Canadian International Council, 2012.

CROSTON, Matthew. Soft Spying: Leveraging Globalization as Proxy Military Rivalry. **International Journal of Intelligence and CounterIntelligence**, v. 28, n. 1, 2015.

DANIELSON, Mark E. A. Economic Espionage: a framework for a workable solution. **Minnesota Journal of Law, Science & Technology**, v. 10, 2008.

D'ASPREMONT, Jean. **Formalism and the Sources of International Law**: a theory of the ascertainment of legal rules. Oxford University Press, 2011.

DEEKS, Ashley. An International Legal Framework for Surveillance. **Virginia Journal of International Law**, v. 55, 2015.

_____. Intelligence Communities, Peer Constraints, and the Law. **Harvard National Security Journal**, v. 7, 2015.

DEMAREST, Geoffrey B. Espionage in International Law. **Denver Journal of International Law and Policy**, v. 24, n. 2, 3, 1996.

DIAMOND, John. **The CIA and the Culture of Failure**: US Intelligence from the End of the Cold War to the Invasion of Iraq. Stanford University Press, 2008.

DROGIN, Bob. **Curveball**. Tradução: Ricardo Gozzi. São Paulo: Novo Conceito, 2008.

DWORKIN, Ronald. A New Philosophy for International Law. **Philosophy and Public Affairs**, v. 41, n. 1, 2013.

_____. **Levando os Direitos a Sério**. Tradução: Nelson Boeira. 1 ed. Martins Fontes, 2002.

_____. **Is Democracy Possible Here?: principles for a new political debate**. Princeton University Press, 2006.

FIDLER, David P. Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies. **American Society of International Law Insights**, v. 17, n. 10, 2013.

_____. Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage. **Arms Control Law**, 11 fev. 2013. Disponível em: <http://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>

FITZMAURICE, Gerald. The general principles of international law considered from the standpoint of the rule of law. **Collected Courses of the Hague Academy of International Law**, 1957.

FORCESE, Craig. Spies Without Borders: International Law and Intelligence Collection. **Journal of National Security Law and Policy**, 2011.

FRANCK, Thomas M. **The Power of Legitimacy among Nations**. Oxford University Press, 1990.

FUKUYAMA, Francis. **The End of History and the Last Man**, The Free Press, 1992.

GARCÍA-MORA, Manuel R. Treason, Sedition and Espionage as Political Offenses under the Law of Extradition. **University of Pittsburgh Law Review**, v. 26, 1964.

GARFINKEL, Simson. **Database Nation**: the death of privacy in the 21st Century. Sebastopol: O'Reilly, 2000.

GENDRON, Angela. Just war, just intelligence: an ethical framework for foreign espionage. **International Journal of Intelligence and CounterIntelligence**, v. 18, n. 3, 2005.

GILBERT, Martin. **A Segunda Guerra Mundial**. Tradução: Ana Luísa Faria; Miguel Serras Pereira. Rio de Janeiro: Casa da Palavra, 2014 [Edição Original de 1989].

GLASER, Charles L. Realists as Optimists: Cooperation as Self-Help. **International Security**, v. 19, n. 3, 1995.

GREENBERG, Lawrence T.; GOODMAN, Seymour E.; SOO HOO, Kevin J. **Information Warfare and International Law**. National Defense University Press, 1998.

GRIFFITHS, Martin. **Fifty Key Thinkers in International Relations**. Routledge, 1999.

GROSS, Ernest A. International Organization and Collective Security: Changing Values and Priorities. **Collected Courses of the Hague Academy of International Law**, 1973.

GROTIUS, Hugo. **The Law of War and Peace**, 1625.

GUZMAN, Andrew T. **How International Law Works**: a rational choice theory. Oxford University Press, 2008.

HANSON, Jon D.; KYSAR, Douglas A. Taking Behavioralism Seriously: The Problem of Market Manipulation. **New York University Law Review**, v. 74, 2008.

HASTEDT, Glenn. **Espionage: a reference handbook**. Santa Barbara: ABC-Clio, 2003.

HAYNES, John Earl; KLHER, Harvey. **Early Cold War Spies**. Cambridge University Press, 2006.

HENKIN, Louis. International Law: Politics, Values and Functions. **Collected Courses of the Hague Academy of International Law**, 1989.

HERMAN, Michael. **Intelligence Power in Peace and War**. Cambridge University Press, 1999.

HERZ, John H. **Political Realism and Political Idealism**: a study in theories and realities. The University of Chicago Press, 2 ed., 1959.

HOLLOWAY, David. **9/11 and the War on Terror**, Edinburgh University Press, 2008.

_____. Stalin and the Bomb: The Soviet Union and Atomic Energy, 1939-1956. **Yale University Press**, 1994.

HUDSON, Manley. **La Cour Permanente de Justice Internationale**. Paris, 1936.

JACKSON, John H. **Sovereignty, the WTO and Changing Fundamentals of International Law**. Cambridge: Cambridge University Press, 2006.

JENNINGS, Robert; WATTS, Arthur [eds.]. *Oppenheim's International Law*, 9 ed., 1992,

JERVIS, Robert. Cooperation under the Security Dilemma, **World Politics**, v. 30, n. 2, 1978.

_____. **Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War**. Cornell University Press, 2010.

JOHNSON, Lock K. [org.] **Handbook of Intelligence Studies**, London: Routledge, 2007.

_____. [org.] **Strategic Intelligence**, 2 vol., Preager Security International, 2007.

KALMO, Hent; SKINNER, Quentin. **Sovereignty in Fragments: the past, present and future of a contested concept**. Cambridge University Press, 2010.

KELSEN, Hans. **Principles of International Law**. Rinehart and Company, 1952.

KENT, Sherman. **Strategic Intelligence for American World Policy**. Princeton University Press, 1949.

KEOHANE; Robert O. International Relations and International Law: Two Optics. **Harvard International Law Journal**, v. 38, n. 2, 1997.

_____. [org.] **Neorealism and its Critics**. Columbia University Press, 1986.

_____.; NYE, Joseph S. **Power and Interdependence**, Little, Brown, 1977.

KESSLER, Ronald. **The Bureau: the secret history of the FBI**. Macmillan, 2016.

KHALIL, Chantal. Thinking Intelligently about Intelligence: a model global framework protecting privacy. **The George Washington International Law Review**, v. 47, 2015.

KISH, John. *International Law and Espionage*. **Martinus Nijhoff Publishers**, 1995.

KITROSSER, Heidi. Free Speech aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information. **Journal of National Security Law & Policy**, v. 6, 2013.

_____. "Macro-Transparency" as Structural Directive: A Look at the NSA Surveillance Controversy. **Minnesota Law Review**, v. 91, pp. 1163-1208, 2007.

KLABBERS, Jan. Clinching the concept of sovereignty: Wimbledon redux. **Austrian Review of International and European Law**, v. 3, 1998.

KNORR, Klaus. Failures in national intelligence estimates: the case of the Cuban missiles. **World Politics**, v. 16, n. 3, 1964.

KORAB-KARPOWICZ, W. Julian. Political Realism in International Relations, **The Stanford Encyclopedia of Philosophy**, 2013. Disponível em: <http://plato.stanford.edu/archives/sum2013/entries/realism-intl-relations/>

_____. The Relative Autonomy of International Law or the Forgotten Politics of Interdisciplinarity. **Journal of International Law & International Relations**, v. 1, 2005.

KOSKENNIEMI, Martti. **From Apology to Utopia: The Structure of International Legal Argument**. Cambridge University Press, 2005.

_____. Law, Teleology and International Relations: An Essay in Counterdisciplinarity. **International Relations**, v. 26, n. 1, 2011.

_____. **The Gentle Civilizer of Nations: the rise and fall of international law 1870-1960**. Cambridge University Press, 2004. p. 475.

KRASKA, James. Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters. **Columbia Journal of Transnational Law**, v. 54, 2015.

KRASNER, Stephen D. **Sovereignty: organized hypocrisy**. Princeton University Press, 1999.

KREPTON, Michael. Looking Back: The 1998 Indian and Pakistani Nuclear Tests. **Arms Control Today**, Arms Control Association, 11 jun. 2008.

KUPERWASSER, Yosef. **Lessons from Israel's Intelligence reforms**, analysis paper, n. 14. The Saban Center at the Brookings Institution, 2007.

LAFOUASSE, M. Fabien. Espionnage en droit international. **Annuaire français de droit international**, v. 47, 2001.

LANDAU, Susan. **Surveillance or Security**. Massachusetts Institute of Technology Press, 2010.

LATHROP, Charles E. **The Literary Spy**. Yale University Press, 2004.

LAUTERPACHT, Hersch. Some Observations on the Prohibition of *Non Liquet* and the Completeness of the Legal Order. *Symbolae Verzijl*, 1958.

LEAL, Fernando. O Formalista Expiatório: leituras impuras de Kelsen no Brasil. **Revista Direito GV**, v. 10, 2014.

LEBOW, Richard Ned. The long peace, the end of the cold war, and the failure of realism. **International Organization**, v. 48, n. 2, 1994.

LEGRO, Jeffrey; MORAVCSIK, Andrew. Is anybody still a realist? **International Security**, v. 24, n. 2, 1999.

LEIGH, Ian. Democratic Control of security and Intelligence Services: a legal framework. In: **Security Sector Reform: Institutions, Society and Good Governance**, Geneva, 2003.

LERNER, K. Lee; LERNER, Brenda Wilmoth. [orgs.] **Encyclopedia of Espionage, Intelligence, and Security**, v. 1. Farming Hills: Thomson Gale, 2004.

LEWIS, James A. **Conflict and Negotiation in Cyberspace**. Washington: Center for Strategic and International Studies, 2013.

LIMA, Humberto Alves de Vasconcelos. A construção do vínculo entre propriedade intelectual e comércio internacional e seus reflexos no Brasil. **Revista Eletrônica Direito e Política**, v. 9, n. 2, 2014. Disponível em: <<http://www6.univali.br/seer/index.php/rdp/article/view/6033>>

_____; CUNHA, Naiana Magrini Rodrigues. O problema da espionagem econômica internacional: seria a Organização Mundial do Comércio o foro adequado para sua apreciação? **Revista de Direito Internacional**, v. 12, n. 2, pp. 92-106, 2014.

LINDSAY, Jon R.; CHEUNG, Tai Ming; REVERON, Derek S. **China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain**. Oxford University Press, 2015.

LOTRIONTE, Catherine. Countering State-Sponsored Cyber Economic Espionage Under International Law. **North Carolina Journal of International Law and Commercial Regulation**, v. XL, 2015

MALANCZUK, Peter. **Akerhurst's Modern Introduction to International Law**, 7 ed., 2002.

MATSUSHITA, Mitsuo; SCHOENBAUM, Thomas J.; MAVROIDIS, Petros C. **The World Trade Organization: Law, Practice and Politics**. Oxford: Oxford University Press, 2006.

MCDUGAL, Myres S.; LASSWELL, Harold D.; REISMAN, W. Michael. The Intelligence Function and World Public Order. **Temple Law Quarterly**, v. 46, n. 3, 1973.

MILANOVIC, Marko. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. **Harvard International Law Journal**, v. 56, n. 1, 2015.

MCGREGOR, James. **China's Drive for 'Indigenous Innovation': A Web of Industrial Policies**. U.S. Chamber of Commerce, Global Intellectual Property Center, 2010.

MEARSHEIMER, John J. **The Tragedy of Great Power Politics**. W. W. Norton & Company, 2001.

MOORE, Adam D. Toward Informational Privacy Rights. **San Diego Law Review**, v. 44, 2007.

MONJE, Scott. **The Central Intelligence Agency: a documentary history**. Greenwood Press, 2008.

MORAN, Jon; PHYTHIAN, Mark. **Intelligence, Security and Policing Post-9/11: The UK's Response to the 'War on Terror'**. Palgrave Macmillan, 2008.

NADER, Ralph; PETKAS, Peter J.; BLACKWELL, Kate [org.] **Whistle Blowing: the report on the conference on professional responsibility**. Grossman Publishers, 1972.

NASSER, Salem Hikmat. *Jus Cogens*: ainda esse desconhecido. **Revista Direito GV**, v. 1, n. 2, 2005.

NEACSU, Mihaela. **Hans J. Morgenthau's Theory of International Relations: Disenchantment and Re-Enchantment**. Palgrave Macmillan, 2009.

NISSEMBAUM, Helen. Protecting Privacy in an Information Age: The Problem of Privacy in Public. **Law and Philosophy**, v. 17, 1998.

NORTH ATLANTIC TREATY ORGANIZATION. **NATO Open Source Intelligence Handbook**, 2001.

_____. **Tallin Manual on the International Law Applicable to Cyber Warfare**, Cambridge: Cambridge University Press, 2013.

O'CONNELL, Anne Joseph. The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World. **California Law Review**, v. 94, 2006.

OLESON, Peter C. **Who Are the Customers for Intelligence?** [draft paper] Disponível em: <[http://www.afio.com/publications/OLESON_Who%20are%20customers%20of%20intel%20\(rev\)_Draft_2014Feb10.pdf](http://www.afio.com/publications/OLESON_Who%20are%20customers%20of%20intel%20(rev)_Draft_2014Feb10.pdf)>

ONUF, Nicholas. **World of Our Making: Rules and Rule in Social Theory and International Relations**, University of South Carolina Press, 1989.

PEYTON, Cooke. Bringing the Spies in from the Cold: Legal Cosmopolitanism and Intelligence Under the Laws of War. **University of San Francisco Law Review**, v. 44, 2010.

PILLAR, Paul R. Intelligence, Policy and the War in Iraq. **Foreign Affairs**, v. 85, n. 2, mar/abr. 2006.

POLLACK, Mark. A. Is International Relations Corrosive of International Law? A reply to Martti Koskeniemi. **Temple International Law and Comparative Law Journal**, v. 27, n. 2, 2013.

POLIDO, Frabício Bertini Pasquot; ANJOS, Lucas Costa dos. [orgs.] **Marco Civil e Governança da Internet: diálogos entre o doméstico e o global**, Universidade Federal de Minas Gerais, 2016.

POSNER, Richard. **Economic Analysis of Law**. New York: Aspen, 5 ed, 1998.

PURVIS, Nigel. Critical Legal Studies in Public International Law. **Harvard International Law Journal**, v. 32, n. 1, 1991.

RADSAN, A. John. The Unresolved Equation of Espionage and International Law. **Michigan Journal of International Law**, v. 28, 2007.

REINARES, Fernando. After the Madrid Bombings: Internal Security Reforms and the Prevention of Global Terrorism in Spain. **Studies in Conflict & Terrorism**, v. 32, n. 5, 2009.

RICHELSON, Jeffrey T. **A Century of Spies: Intelligence in the Twentieth Century**. Oxford University Press.

ROSEN, Jeffrey. **The Unwanted Gaze: The Destruction of Privacy in America**. New York: Vintage, 2001.

ROSS, Alf. **A Textbook of International Law**. Longmans, 1947.

SAMORE, Gary [org]. **Decoding the Iran Nuclear Deal**. Harvard Kennedy School, Belfer Center for Science and International Affairs, 2015.

SARAT, Austin [org.] **A World Without Privacy: What Law Can and Should Do?** Cambridge University Press, 2015.

SCHACHTER, Oscar. General Course in Public International Law. **Collected Courses of the Hague Academy of International Law**, 1982.

SCHEUERMAN, William E. **The Realist Case for Global Reform**, Polity Press, 2011.

SCHMITT, Carl. **Political Theology: Four Chapters on the Concept of Sovereignty**. Tradução: George Schwab, University of Chicago Press, 1985.

_____. **The Concept of the Political**: expanded edition. Tradução: George Schwab. The University of Chicago Press, [edição original: 1932], 2007.

SCHUTTER, Olivier De. **International Human Rights Law**, Cambridge University Press, 2010.

SCOTT, Roger D. Territorially Intrusive Intelligence Collection and International Law. **The Air Force Law Review**, 1999.

SHAPIRO, Scott J. **Legality**. The Belknap Press of Harvard University Press, 2011.

SHAW, Malcolm N. **International Law**. Cambridge University Press, 6 ed., 2008.

SKINNER, Christina Parajon. An International Law Response to Economic Cyber Espionage. **Connecticut Law Review**, v. 46, n. 4, 2014.

SLAUGHTER, Anne-Marie. **A New World Order**. Princeton University Press, 2004.

_____. International Law and International Relations. **Collected Courses of the Hague Academy of International Law**, 2000.

_____. International Law in a World of Liberal States. **European Journal of International Law**, v. 6, 1995.

_____; TULUMELLO, Andrew S.; WOOD, Stepan. International Law and International Relations Theory: A New Generation of Interdisciplinary Scholarship. **The American Journal of International Law**, v. 92, n. 3, 1998.

SNYDER, Jack. **Myths of Empire: Domestic Politics and International Ambition**. Cornell University Press, 1991.

SOLOVE, Daniel J. **Nothing to Hide: The False Tradeoff between Privacy and Security**, Yale University Press, 2011.

STANGER, Roland J. (Org.) **Essays on Espionage and International Law**, Ohio University Press, 1962.

STEELE, Robert David. **The Open-Source Everything Manifesto: Transparency, Truth and Trust**. Berkeley: Evolver Editions, 2012.

STOYCHEFF, Elizabeth. Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. **Journalism & Mass Communication Quarterly**, 2016.

SULMASY, Glenn; YOO, John. Counterintuitive: Intelligence Operations and International Law. **Michigan Journal of International Law**, v. 28, 2006-2007.

SUSKIND, Ron. **The One Percent Doctrine**. Simon & Schuster, 2006.

TOMUSCHAT, Christian. Obligations arising for States without or against their will. **Collected Courses of the Hague Academy of International Law**, 1993.

TRINDADE, Antônio Augusto Cançado. International Law for Humankind: Towards a New *Jus Gentium*. **Collected Courses of the Hague Academy of International Law**, part II, 2005.

TUNKIN, Grigoriĭ Ivanovich. **Theory of international law**. Harvard University Press, 1974.

UNGER, Roberto Mangabeira. The Critical Legal Studies Movement. **Harvard Law Review**, v. 96, n. 3, 1983.

VOLLER, Yaniv. After the Arab Spring: power shift in the Middle East?: turmoil and uncertainty: Israel and the New Middle East. **IDEAS Reports**, London School of Economics, 2012.

WALDRON, Jeremy. Security and Liberty: The Image of Balance. **The Journal of Political Philosophy**, v. 11, n. 2, 2003.

WALT, Stephen M. **The Origins of Alliances**, Cornell University Press, 1990.

WALTZ, Kenneth. Structural Realism after the Cold War. **International Security**, v. 25, n. 1, 2000.

_____. **Theory of International Politics**. Addison-Wesley, 1979.

WAXMAN, Matthew C. Self-Defense and the Limits of WMD Intelligence. *In: Koret-Taube Task Force on National Security and Law*, Hoover Institution, Stanford University, 2010.

WEIL, Prosper. Towards Relative Normativity in International Law? **The American Journal of International Law**, v. 77, 1983.

_____. "The Court Cannot Conclude Definitively...": *non liquet* revisited. **Columbia Journal of Transnational Law**, v. 36, 1997.

WENDT, Alexander. Collective identity formation and the international state. **American Political Science Review**, v. 88, 1994.

WILLIAMS, Michael C. **Realism Reconsidered: The Legacy of Hans Morgenthau in International Relations**, Oxford University Press, 2007.

WILLIAMS, Robert D. (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action. **The George Washington Law Review**, v. 79, 2011.

WILLIAMS, Robert E. Jr.; VIOTTI; Paul R. [orgs.] **Arms Control: History, Theory and Policy**. Praeger Security International, 2 vols., 2012.

WINKS, Robin W. **Cloak and Gown: Scholars in the Secret War, 1939–1961**. New York: William Morrow, 1987.

WOLTER, Detlev. **Common Security in Outer Space and International Law**. United Nations Institute for Disarmament Research, 2005.

WRANGE, Pål. Intervention in National and Private Cyber Space and International Law. *In: The Fourth Biennial Conference of the Asian Society of International Law*, Delhi, 14-16 novembro 2013.

WRIGHT, Peter. **Spy Catcher**. Australia: William Heinemann Publishers, 1987.

YOO, John. **The Powers of War and Peace: The Constitution and Foreign Affairs after 9/11.** The University of Chicago Press, 2005.

YU, Rong; GUANGQIAN, Peng. Nuclear No-First-Use Revisited. **China Security**, v. 5, n. 1, 2009.

XUETONG, Yan. Political Leadership and Power Redistribution. **The Chinese Journal of International Politics**, v. 9, n. 1, 2016.

ZIOLKOWSKI, Katharina. **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy.** NATO Cooperative Cyber Defence Centre of Excellence, Tallin, 2013.

ZUHUR, Sherifa. **Precision in the Global War on Terror: Inciting Muslims through the War of Ideas.** Strategic Studies Institute, 2008.

2. Documentos e sites oficiais de Estados e Organizações Internacionais

ADMINISTRACIÓN DE JUSTICIA (Espanha). **Juzgado Central de Instrucción nº 6**, 10 abr. 2006. p. 1412. Disponível em: <http://www.elmundo.es/documentos/2006/04/11/autohtml/index.html?cual=1412>

BRASIL. **Discurso de S.E. a Senhora Dilma Rousseff, Presidenta (sic) da República Federativa Do Brasil, na Abertura do Debate Geral da 68ª Sessão da Assembleia Geral das Nações Unidas**, Nova York, 24 set. 2013. Disponível em: <http://www.onu.org.br/img/2013/09/Brasil-UNGA.pdf>

BEST JR., Richard A.; CUMMING, Alfred. Open Source Intelligence (OSINT): Issues for Congress. **Congressional Research Service**, 05 dez. 2015.

CENTRAL INTELLIGENCE AGENCY (Estados Unidos). **A Compendium of Analytic Tradecraft Notes**, v. 1, 1997.

_____. **Freedom of Information Act Electronic Reading Room.** Disponível em: <http://www.foia.cia.gov/>

_____. **National Intelligence Daily**, 7 april 1994. p. 12. Disponível em: http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000638200.pdf

_____. **Notes on the Critic System.** Disponível em: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol4no2/html/v04i2a03p_0001.htm

_____. **Offices of CIA.** Disponível em: <https://www.cia.gov/offices-of-cia/>

_____. **Our First Line of Defense: Presidential Reflections on US Intelligence**, Center for the Study of Intelligence 1996.

_____. **Some Likely Intelligence Questions for the 1980's**. Disponível em: <http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0001246423.pdf>

_____. **The World Factbook**. Disponível em: <<https://www.cia.gov/library/publications/the-world-factbook/>>

CLAPPER, James. **DNI Statement on Recent Unauthorized Disclosures of Classified Information, Office of the Director of National Intelligence**, 06 jun. 2013. Disponível em: <<http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information>>

CLARKE Richard A.; MORELL, Michael J.; STONE, Geoffrey R.; SUNSTEIN, Cass R.; SWIRE, Peter. **Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies**, 12 dez. 2013. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>

COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION, THE (Estados Unidos). **Report to the President of the United States**, 31 mar. 2005. Disponível em: <https://fas.org/irp/offdocs/wmd_report.pdf>

CONGRESSIONAL RESEARCH SERVICE (Estados Unidos). **The U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review: An Overview**, 24 jan. 2007.

COUNCIL OF EUROPE. **Democratic and effective oversight of national security services**, 2015.

DATA Gathering. **Intelligence.gov**, Disponível em: <<http://www.intelligence.gov/mission/data-gathering.html>>

DEPARTMENT OF DEFENSE (Estados Unidos). **Dictionary of Military and Associated Terms**. 2015. Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>

ELSEA, Jennifer K. Intelligence Identities Protection Act. **Congressional Research Service**, 10 abril 2013.

EUROPEAN PARLIAMENT. **Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)**, 2001.

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES. **Administration Strategy on Mitigating The Theft of U.S. Trade Secrets**, fev. 2013. Disponível em: <https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>

FEDERAL BUREAU OF INVESTIGATION (Estados Unidos). **Wanted by the FBI: Cyber's Most Wanted**. Disponível em: <<https://www.fbi.gov/wanted/cyber>>

GATES, Robert. **Guarding Against Politicization: a message to analysts**, 16 mar. 1992. Disponível em: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/volume-36-number-1/html/v36i1a01p_0001.htm>

INTELLIGENCE AND SECURITY COMMITTEE (Reino Unido). **Could 7/7 Have Been Prevented?** Review of the Intelligence on the London Terrorist Attacks on 7 July 2005, mai. 2009.

INTERNATIONAL TELECOMMUNICATION UNION. **Statistics**. Disponível em: <<http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>>

JOINT COMMITTEE ON ATOMIC ENERGY (Estados Unidos). **Soviet Atomic Espionage**, 1951. Disponível em: <<http://archive.org/stream/sovietatomicespi1951unit#page/n4/mode/1up>>

MANNINGHAM-BULLER, Elizabeth Lydia. **The international terrorist threat and the dilemmas in countering it**. Discurso em Ridderzaal, Binnenhof, Haia, Holanda, 2005. Disponível em: <<https://www.mi5.gov.uk/fr/node/406>>

NATIONAL SECURITY AGENCY. **UKUSA Agreement Release 1940-1956**. Disponível em: <https://www.nsa.gov/public_info/declass/ukusa.shtml>

NATIONAL SECURITY ARCHIVE, THE (Estados Unidos). **Brazil Marks 40th Anniversary of Military Coup Declassified Documents Shed Light on U.S. Role**. Disponível em: <<http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB118/index.htm#docs>>

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (Estados Unidos). **Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution**, 06 jan. 2017. Disponível em: <<https://assets.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf>>

_____. **Intelligence community directive 204: National Intelligence Priorities Framework**. Disponível em: <<http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf>>

_____. **Members of the IC**. Disponível em: <<http://www.dni.gov/index.php/intelligence-community/members-of-the-ic>>

_____. **Worldwide Threat Assessment of the US Intelligence Community**, 26 fev. 2015.

_____. **U.S. Intelligence Community Budget**. Disponível em: <<http://www.dni.gov/index.php/resources/intelligence-community-budget>>

PIETRASANTA, Sébastien M. Rapport Fait au Nom de la Commission D'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015. **Assemblée Nationale**, 5 jul. 2016. Disponível em: <<http://www.assemblee-nationale.fr/14/pdf/rap-eng/r3922-t1.pdf>>

POSNER, Eric A. **Statement to the Privacy & Civil Liberties Oversight Board**, 14. mar. 2014. Disponível em: <<https://www.pclob.gov/library/20140319-Testimony-Posner.pdf>>

UNITED NATIONS. Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, **International Law Commission**, 2001. Disponível em: <http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>

_____. Fragmentation of International Law: Difficulties Arising From the Diversification and Expansion of International Law. **International Law Commission**, 2006. Disponível em: <http://legal.un.org/ilc/documentation/english/a_cn4_l682.pdf>

_____. Preliminary report on International liability for injurious consequences arising out of acts not prohibited by international law, **International Law Commission**, 1980. Disponível em: <http://legal.un.org/docs/?path=../ilc/documentation/english/a_cn4_334.pdf&lang=EFS>

_____. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. **Human Rights Council**, Resolution 28/16, 24 mar 2015. Disponível em: <http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/28/L.27>

_____. **Security Council Imposes Additional Sanctions on Iran, Voting 12 in Favour to 2 Against, with 1 Abstention**. Press Release. 9 jun. 2010. Disponível em: <<http://www.un.org/press/en/2010/sc9948.doc.htm>>

_____. **Security Council Veto List**. Disponível em: <<http://research.un.org/en/docs/sc/quick>>

_____. The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art. 17), **Human Rights Committee**, General Comment nº 16, item 8, 8 abr. 1988.

UNITED NATIONS GENERAL ASSEMBLY. **Charter of Economic Rights and Duties of States**, 1974.

_____. **Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations**, A/RES/25/2625, 24 out. 1970.

_____. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, Disponível em: <https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf>

_____. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723, Disponível em: <<https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>>

_____. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. A/69/397, 23 set. 2014. Disponível em <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/pdf/N1454519.pdf?OpenElement>>

_____. Report of the Special Rapporteur on the right to privacy. A/HRC/31/64, **Human Rights Council**. 8 mar. 2016. Disponível em: <<http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>>

_____. **The right to privacy in the digital age**. Resolution 68/167, 21 jan. 2014. Disponível em: <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>

_____. **The right to privacy in the digital age**: Report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/27/37, 30 jun. 2014. Disponível em: <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/088/54/pdf/G1408854.pdf?OpenElement>>

UNITED STATES DEPARTMENT OF JUSTICE. **A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen**, ago. 2013. Disponível em: <<https://oig.justice.gov/special/0308/final.pdf>>

_____. **U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage**, 19 maio 2014. Disponível em: <<http://www.justice.gov/opa/pr/2014/May/14-ag-528.html>>

UNITED STATES DEPARTMENT OF STATE. **Joint Comprehensive Plan of Action**, 2015. Disponível em: <<http://www.state.gov/documents/organization/245317.pdf>>

UNITED STATES OF AMERICA. **The 9/11 Commission Report**, National Commission on Terrorists Attacks Upon the United States, 2004.

_____. **The National Security Strategy of the United States of America**, The White House, 2002. Disponível em: <<http://www.state.gov/documents/organization/63562.pdf>>

3. Documentos e sites de empresas e organizações privadas

BERGEN, Peter; STERMAN, David; SCHNEIDER, Emily; CAHALL, Bailey. Do NSA's Bulk Surveillance Programs Stop Terrorists? **New America Foundation**, jan. 2014. Disponível em: <https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf>

BERTON, Beatrice. The dark side of the web: ISIL's one-stop shop? **EUISS Alert**, Institute for Security Studies, European Union, v. 30, 2015. Disponível em: <http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf>

ELETRONIC INFORMATION PRIVACY CENTER. **Foreign Intelligence Surveillance Act Court Orders – 1979-2015**. Disponível em: <<https://epic.org/privacy/surveillance/fisa/stats/default.html>>

FEDERATION OF AMERICAN SCIENTISTS. **IMINT Gallery**. Disponível em: <<http://fas.org/irp/imint/>>

_____. **Intelligence Resource Program: Intelligence Budget Data**. Disponível em: <<http://fas.org/irp/budget/>>

FIREEYE. **Red Line Drawn: China recalculates its use of cyber espionage**, jun. 2016. Disponível em: <<https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf>>

ISMI, Asad. Canadian government spies on Brazil – and its own citizens. **Canadian Center for Policy Alternatives**, 1 nov. 2013. Disponível em: <<https://www.policyalternatives.ca/publications/monitor/massive-secret-surveillance-canada>>

MANDIANT. **APT1: Exposing One of China's Cyber Espionage Units**, 2013. Disponível em: <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>

NELSON, Raymond. Scientific Basis for Polygraph Testing. **Polygraph**, v. 44, n. 1, 2015. Disponível em:

<https://apoa.memberclicks.net/assets/docs/nelson_2015_scientific_basis_for_polygraph.pdf>

NORTON. **The Stuxnet Worm**. Disponível em: <<http://us.norton.com/stuxnet>>

PRIVACY INTERNATIONAL. **Metadata**. Disponível em: <<https://www.privacyinternational.org/node/53>>

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE. **SIPRI Military Expenditure Database**. Disponível em: <<https://www.sipri.org/databases/milex>>

TOR PROJECT. Disponível em: <www.torproject.org>

WORLD PRIVACY FORUM. **What Information Do Data Brokers Have on Consumers, and How Do They Use It?** Testimony of Pam Dixon Executive Director, World Privacy Forum, before the Senate Committee on Commerce, Science, and Transportation, 18 dez. 2013. Disponível em: <http://www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf>

4. Legislação e decisões judiciais

ANTI-BALLISTIC MISSILE TREATY, 1972.

AUSTRALIA. **Intelligence Services Act**, 2001.

BRASIL. **Lei 9.883/1999**.

_____. **Lei 12.527/2011**.

_____. **Decreto 4.376/2002**.

CANADA. **Security Intelligence Service Act**, 1985.

CARTA DAS NAÇÕES UNIDAS, 1945.

CONVENÇÃO AMERICANA SOBRE OS DIREITOS HUMANOS, 1969.

CONVENÇÃO DE BUDAPESTE SOBRE CRIMES CIBERNÉTICOS, 2001.

CONVENÇÃO EUROPEIA DOS DIREITOS HUMANOS, 1950.

CONVENÇÕES DE GENEBRA, 1949.

CONVENÇÕES DE HAIA, 1899, 1907.

DECLARAÇÃO DE BRUXELAS, 1874.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948.

EUROPEAN COURT OF HUMAN RIGHTS. **Internet: case-law of the European Court of Human Rights**, jun 2015. Disponível em: <http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf>

_____. **Klass and Others v. Germany**, Processo nº 5029/71, julgamento em 6 set. 1978.

_____. **Roman Zakharov v. Russia**, Processo nº 47143/06, julgamento em 4 dez. 2015.

_____. **Rotaru v. Romania**, Processo nº 28341/95, julgamento em 4 maio 2000.

_____. **Szabó and Vissy v. Hungary**. Processo nº 37138/14, julgamento em 12 jan. 2016.

GENERAL AGREEMENT ON TARIFFS AND TRADE, 1994.

HUNGARY. **Act on the National Security Services**, 1995.

INTER-AMERICAN COURT OF HUMAN RIGHTS. **Case of Escher et al. v. Brazil**, julgamento em 6 jul. 2009.

INTERNATIONAL COURT OF JUSTICE. **Case Concerning Military and Paramilitary Activities in and Against Nicaragua**, 27 jun 1986.

_____. **Legality of the threat or use of nuclear weapons**, advisory opinion, 8 July 1996.

_____. **Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia)**, Application, 17 dez. 2013.

_____. **to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia)**. Application and Request for the indication of provisional measures, 3 mar. 2014.

ORGANIZAÇÃO MUNDIAL DO COMÉRCIO. **Acordo Sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio**, 1994. art. 39 (2).

PACTO INTERNACIONAL DE DIREITOS CIVIS E POLÍTICOS, 1966.

PERMANENT COURT OF INTERNATIONAL JUSTICE. **Publications of the Permanent Court of International Justice: the case of the S.S. "Lotus"**, 1927. p. 18. Disponível em: <http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf>

STRATEGIC ARMS LIMITATIONS TREATY I/II, 1972, 1979.

UNITED KINGDOM. **Anti-terrorism, Crime and Security Act**, 2001.

_____. **Terrorism Act**, 2006.

UNITED STATES CONGRESS. Congress.gov. H.R. 3162 - USA PATRIOT ACT. <<https://www.congress.gov/bill/107th-congress/house-bill/3162/text>>

UNITED STATES OF AMERICA. **Economic Espionage Act**, 1996

_____. **Executive Order nº 12.333**

_____. **FISA Amendments Act**, 2008.

_____. **Foreign Intelligence Surveillance Act**, 1978.

_____. **Freedom of Information Act**, 1966.

_____. **Intelligence Reform and Terrorism Prevention Act**, 2004.

_____. **Protect America Act**, 2007.

5. Imprensa

6,000 Reported Killed in Burundi Coup. **The New York Times**, 23 ago. 1996. Disponível em: <http://www.nytimes.com/1996/08/23/world/6000-reported-killed-in-burundi-coup.html>>

ALLEN, Ian. Switzerland to probe claims it was spied on by US, German agencies. **Intelnews.org**, 28 maio 2015. Disponível em: <http://intelnews.org/2015/05/28/01-1705/>>

———. Belgium launches official probe into alleged German-US espionage. **Intelnews.org**, 8 jun. 2015. Disponível em: <http://intelnews.org/2015/06/08/01-1710/>>

ANDREWS, Wilson; LINDEMAN, Todd. \$ 52.6 Billion: The Black Budget. **The Washington Post**, 29. ago. 2013. Disponível em: <http://www.washingtonpost.com/wp-srv/special/national/black-budget/>>

BALL, James. NSA monitored calls of 35 world leaders after US official handed over contacts. **The Guardian**, 25 out. 2013. Disponível em: <http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>>

_____; MACASKILL, Ewen. Portrait of the NSA: no detail too small in quest for total surveillance. **The Guardian**, 2 nov. 2013. Disponível em: <https://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance>>

BARNEA, Nahum; SHIFFER, Shimon. “Netanyahu has caused Israel the most strategic damage on Iran”. **Ynetnews.com**, 27 fev. 2015. Disponível em: <http://www.ynetnews.com/articles/0,7340,L-4631634,00.html>>

BARRET, David. One surveillance camera for every 11 people in Britain, says CCTV survey. **The Telegraph**, 10 jul. 2013. Disponível em: <http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html>>

BENJAMIN Netanyahu Speech to Congress 2015. **The New York Times**, Disponível em: <https://www.youtube.com/watch?v=wRf1cdw4IAY>>

BEVINS, Vincent. Why did Brazil's President Change Her Tune on Spying? **Foreign Policy**, 16 jun. 2015. Disponível em: <http://foreignpolicy.com/2015/06/16/brazil-nsa-spying-surveillance-economy-dilma-rousseff-barack-obama/>>

BORGER, Julian. French and Belgian intelligence knew Paris attackers had jihadi backgrounds. **The Guardian**, 16 nov. 2015. Disponível em: <http://www.theguardian.com/world/2015/nov/16/french-and-belgian-intelligence-knew-paris-attackers-had-jihadi-backgrounds>>

BURGESS, Matt. UN privacy chief: UK surveillance bill is 'worse than scary'. **Wired**, 10 nov. 2015. Disponível em: <<http://www.wired.co.uk/news/archive/2015-11/10/surveillance-investigatory-powers-scary-joseph-cannataci>>

BUSH says he signed NSA wiretap order. **CNN International**, 18 dez. 2015. Disponível em: <<http://edition.cnn.com/2005/POLITICS/12/17/bush.nsa/>>

CHABROW, Eric. The Real Aim of the U.S. Indictment of Chinese. **Bank Info Security**, 20 maio 2014. Disponível em: <<http://www.bankinfosecurity.com/real-aim-us-indictment-chinese-a-6854/op-1>>

CUTHBERTSON, Anthony. PhD student forced to remove all WikiLeaks references from her dissertation. **International Business Times**, 10 set. 2015. Disponível em: <<http://www.ibtimes.co.uk/phd-student-forced-remove-all-wikileaks-references-her-dissertation-1519172>>

DENMARK is one of the NSA's '9-Eyes'. **Chp Post Online**, 4 nov. 2013. Disponível em: <<http://cphpost.dk/news/international/denmark-is-one-of-the-nsas-9-eyes.html>>

DORLING, Philip. Singapore, South Korea revealed as Five Eyes spying partners. **The Sydney Morning Herald**, 25 nov. 2013. Disponível em: <<http://www.smh.com.au/technology/technology-news/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html>>

ENTOUS, Adam. Israel Spied on Iran Nuclear Talks With U.S. **The Washington Post**, 23 mar. 2015. Disponível em: <<http://www.wsj.com/articles/israel-spied-on-iran-talks-1427164201>>

ESPIONNAGE Élysée. **Wikileaks**, 23 jun. 2015. Disponível em <<https://www.wikileaks.org/nsa-france/spyorder/>>

[FULL] Colin Powell's Presentation to the UN Security Council on Iraq's WMD Program. **Youtube**, Disponível em: <<https://www.youtube.com/watch?v=ErIDSJHRVMA>>

FITSANAKIS, Joseph. Conflicting details on Iranian nuclear negotiator arrested for espionage. **Intelnews.org**, 30 ago. 2016. Disponível em: <<https://intelnews.org/tag/iranian-nuclear-program/>>

_____. "We killed Iranian scientist" claims Israel intel source. **Intelnews.org**, 03 ago. 2011. Disponível em: <<http://intelnews.org/2011/08/03/01-778/>>

FITZ-MORRIS, James. Why would Canada spy on Brazil mining and energy officials? **CBC News**, 09 out. 2013. Disponível em: <<http://www.cbc.ca/news/politics/why-would-canada-spy-on-brazil-mining-and-energy-officials-1.1931465>>

GELLMAN, Barton; NAKASHIMA, Ellen. U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show. **The Washington Post**, 30 ago. 2013. Disponível em: <https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html>

GERMAN 'Spying' prompts Austria complaint. **BBC News**, 5 maio 2015. Disponível em: <<http://www.bbc.com/news/world-europe-32596510>>

GERTZ, Bill. China's armed drones appear built from stolen data from US cyber intrusions. **Asia Times**, 29 dez. 2015. Disponível em: <<http://atimes.com/2015/12/chinas-armed-drones-appear-built-from-stolen-data-from-us-cyber-intrusions/>>

GOLDSMITH, Jack. The NYT on NSA's Huawei Penetration. **Lawfare**, 22 mar. 2014. Disponível em: <<https://www.lawfareblog.com/nyt-nsas-huawei-penetration-updated>>

GREENWALD, Glenn. **Sem lugar para se esconder**. Tradução: Fernanda Abreu. Sextante, 2014.

GREENWALD, Glenn. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. **The Guardian**, 31 jul. 2013. Disponível em: <<http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>>

_____; FISHMAN, Andrew. Netanyahu's Spying Denials Contradicted by Secret NSA Documents. **The Intercept**, 25 mar. 2015. Disponível em: <<https://theintercept.com/2015/03/25/netanyahus-spying-denial-directly-contradicted-secret-nsa-documents/>>

_____; GRIM, Ryan; GALLAGHER, Ryan. Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'. **The Huffington Post**, 26 nov. 2013. Disponível em: <http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html>

_____; HUSSEIN, Murtaza. Meet the muslim-american leaders the FBI and NSA have been spying on. **The Intercept**, 9 jul. 2014. Disponível em: <<https://theintercept.com/2014/07/09/under-surveillance/>>

_____; MACKASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**, 7 jul. 2013. Disponível em: <<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>>

GRIFFIN, Andrew. France state of emergency declared for three months, allowing authorities to shut down websites and giving police sweeping new powers. **The Independent**, 19 nov. 2015. Disponível em: <<http://www.independent.co.uk/news/world/europe/france-state-of-emergency-declared-for-three-months-allowing-authorities-to-shut-down-websites-and-a6740886.html>>

HAMILOS, Paul; TRAN, Mark. 21 guilty, seven cleared over Madrid train bombings, **The Guardian**, 31. Out. 2007. Disponível em: <<http://www.theguardian.com/world/2007/oct/31/spain.marktran>>

HANS Blix Briefing to the Security Council. **The Guardian**, 14 fev. 2003. Disponível em: <<http://www.theguardian.com/world/2003/feb/14/iraq.unitednations1>>

HINNANT, Lori; DAHLBURG, John-Thor. 'Let's be honest, we eavesdrop too': former French foreign minister on NSA spying claims. CTV News, 23 out. 2013. Disponível em: <<http://www.ctvnews.ca/sci-tech/let-s-be-honest-we-eavesdrop-too-former-french-foreign-minister-on-nsa-spying-claims-1.1509912>>

HOPKINS, Nick. UK gathering secret intelligence via covert NSA operation. **The Guardian**, 7 jun. 2013. Disponível em: <<http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism>>

HUANG, Yufan. Q. and A.: Yan Xuetong Urges China to Adopt a More Assertive Foreign Policy. **The New York Times**, 9. fev. 2016. Disponível em: <http://www.nytimes.com/2016/02/10/world/asia/china-foreign-policy-yan-xuetong.html?_r=0>

IRAN arrests nuclear deal negociator on spying charges. **BBC News**, 28 ago. 2016. Disponível em: <<http://www.bbc.com/news/world-middle-east-37209945>>

IRAN nuclear deal: Key details. **BBC News**, 16 jan. 2016. Disponível em: <<http://www.bbc.com/news/world-middle-east-33521655>>

SIKOFF, Michael. NSA chief: 'Paris would not have happened' without encrypted apps. **Yahoo! Politics**, 17 fev. 2016. Disponível em: <<https://www.yahoo.com/politics/nsa-chief-paris-would-not-have-happened-without-184040933.html>>

KELLEY, Michael B. The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. **Business Insider**, 20 nov. 2013. Disponível em: <<http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11>>

KNIGHT, Ben. Germany reacts to 'double agent' scandal. **DW**, 07 jul. 2014. Disponível em: <<http://dw.com/p/1CXmf>>

KORNBLUT, Anne E. and BENDER, Bryan. Cheney link of Iraq, 9/11 challenged. **The Boston Globe**, 16 ago. 2003. Disponível em: <http://www.boston.com/news/nation/articles/2003/09/16/cheney_link_of_iraq_911_challenged>

LESWING, Kif. The FBI says it has hacked into the San Bernardino shooter's phone without Apple's help. **Business Insider**, 28. Mar. 2016. Disponível em: <<http://www.businessinsider.com/the-government-is-reportedly-ending-its-quest-to-have-apple-help-it-access-data-on-an-encrypted-iphone-2016-3>>

LITHWICK, Dahlia; VLADECK, Steve. Taking the "Meh" out of Metadata. **Slate**, 22 nov. 2013. Disponível em: <http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html>

LUCE, Dan De; GROLL, Elias. In Brussels Attacks, Chronicle of a Disaster Foretold. **Foreign Policy**, 22 mar. 2016. Disponível em: <<http://foreignpolicy.com/2016/03/22/in-brussels-attacks-chronicle-of-a-disaster-foretold/>>

MAYER, Jane. What's the Matter with Metadata? **The New Yorker**, 6 jun. 2013. Disponível em: <<http://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata>>

MAZZETTI, Mark. U.S. Aides Believe China Examined Stealth Copter. **The New York Times**, 14 ago. 2011. Disponível em: <<http://www.nytimes.com/2011/08/15/world/asia/15copter.html>>

MORGENTHAU, Hans J. "We Are Deluding Ourselves in Viet-Nam", **New York Times Magazine**, 18 abr. 1965.

NAKASHIMA, Ellen; MUFSON, Steven. The U.S. and China agree not to conduct economic espionage in cyberspace. **The Washington Post**, 25 set. 2015. Disponível em: <<https://www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to>>

conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html?tid=sm_fb>

NORTH Korea's 'biggest' nuclear test sparks global outrage. **BBC News**, 9 set. 2016. Disponível em: <<http://www.bbc.com/news/world-asia-37317782>>

NSA'S Global Interception Network. **Electropaces.net**, 03 dez. 2013. Disponível em: <<http://electropaces.blogspot.com.br/2013/12/nsas-global-interception-network.html>>

NSA Prism Program Slides. **The Guardian**, Disponível em: <<http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>>

NSA Targets World Leaders for US Geopolitical Interests. **Wikileaks**, Disponível em: <<https://www.wikileaks.org/nsa-201602/>>

OLTERMANN, Philip. ACKERMAN, [Spencer](#). Germany asks top US intelligence official to leave country over spy row. **The Guardian**, 10 jul. 2014. Disponível em: <<http://www.theguardian.com/world/2014/jul/10/germany-asks-top-us-intelligence-official-spy-row>>

PETROBRAS foi espionada pelos EUA, apontam documentos da NSA. **Fantástico**, 08 set. 2013. Disponível em: <<http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html>>

RAVIV, Dan. U.S. pushing Israel to stop assassinating Iranian nuclear scientists. **CBS News**, 1 mar. 2014. Disponível em: <<http://www.cbsnews.com/news/us-pushing-israel-to-stop-assassinating-iranian-nuclear-scientists/>>

RISEN, James; LICHTBLAU, Eric. Bush Lets U.S. Spy on Callers Without Courts. **The New York Times**, 16 dez. 2015. Disponível em: <http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0>

ROBERTS, Dan. Brazilian president's visit to US will not include apology from Obama for spying. **The Guardian**, 30 jun. 2015. Disponível em: <<http://www.theguardian.com/world/2015/jun/30/brazil-dilma-rousseff-obama-nsa-spying-apology>>

_____; GOLDENBERG, Suzanne. US-China summit ends with accord on all but cyber-espionage. **The Guardian**, 10 jun. 2013. Disponível em: <<http://www.theguardian.com/world/2013/jun/09/us-china-summit-barack-obama-xi-jinping>>

RODRIGUEZ, Gabriel. Edward Snowden Interview Transcript. **Policymic**, 9 jun. 2013. Disponível em: <<http://www.policymic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism>>

ROGIN, Josh. NSA Chief: Cybercrime constitutes the greatest transfer of wealth in history. **Foreign Policy**, 9 jul. 2012. Disponível em: <http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history>

SANGER, David E. Obama Order Sped Up Wave of Cyberattacks Against Iran. **The New York Times**, 1 jun. 2012. Disponível em: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=4&_r=1&hp>

_____; PERLROTH, Nicole. N.S.A. Breached Chinese Servers Seen as Security Threat. **The New York Times**, 22 mar. 2014. Disponível em: <<http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?hp&r=0>>

_____; SHANKER, Thom. N.S.A. Devises Radio Pathway Into Computers. **The New York Times**, 14 jan. 2014. <<http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html>>

SCHMITT, Eric. U.S. Officials Met With Belgians on Security Concerns Before Attacks. **The New York Times**, 4 abr. 2016. Disponível em: <<http://www.nytimes.com/2016/04/05/world/europe/us-security-brussels-attacks>>

SHORROCK, Tim. U.S. Intelligence is More Privatized than ever before. **The Nation**, 16 set. 2015. Disponível em: <<http://www.thenation.com/article/us-intelligence-is-more-privatized-than-ever-before/>>

SILVEIRA, Virgínia. Governo brasileiro assina contrato da compra de 36 caças suecos Gripen. **Valor Econômico**, 27 out. 2014. Disponível em: <<http://www.valor.com.br/empresas/3750194/governo-brasileiro-assina-contrato-da-compra-de-36-cacas-suecos-gripen>>

STATISTA: The Statistic Portal. **Cumulative daily mobile message volume of WhatsApp messenger as of April 2014 (in billions)**. Disponível em: <<http://www.statista.com/statistics/258743/daily-mobile-message-volume-of-whatsapp-messenger/>>

TARGETING Huawei: NSA Spied on Chinese Government and Networking Firm. **Spiegel Online International**, 22 mar. 2014. Disponível em: <<http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html>>

'THAT'S Just Not Done': Merkel Comments on Spying Allegations. **Spiegel Online International**, 24 out. 2013. Disponível em: <<http://www.spiegel.de/international/germany/merkel-comments-on-allegations-the-us-spied-on-her-cell-phone-a-929870.html>>

THE LONG, dark war. **The Economist**, 31 jul. 2008. Disponível em: <<http://www.economist.com/node/11837595>>

THE NSA responds to Edward Snowden's TED Talk. **TED**, mar. 2014. Disponível em: <http://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk/transcript?language=en#t-509180>

TRACKING a suspect by mobile phone. **BBC News**. Disponível em: <<http://news.bbc.co.uk/2/hi/technology/4738219.stm>>

TRANSCRIPT of President Obama's Jan. 17 speech on NSA reforms. **The Washington Post**, 17 jan. 2014. Disponível em: <http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html>

URQUHART, Conal. Israel government 'reckless and irresponsible' says ex-Mossad chief. **The Guardian**, 3 jun. 2011. Disponível em: <<http://www.theguardian.com/world/2011/jun/03/israel-government-reckless-mossad-chief>>

VALLE, Sabrina; BAHNEMANN, Wellington; CIARELLI, Mônica. Sem disputa, Petrobras vence leilão de Libra com Shell, Total e duas chinesas. **Agência Estado**, 21 out. 2013. Disponível em: <<http://economia.estadao.com.br/noticias/geral,sem-disputa-petrobras-vence-leilao-de-libra-com-shell-total-e-duas-chinesas,168014e>>

VEJA os documentos ultrassecretos que comprovam espionagem a Dilma. **Fantástico**, 02 set. 2013. Disponível em: <<http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html>>

WINTER, Brian. ENFOQUE - Como a espionagem dos EUA custou à Boeing um contrato multibilionário. **Reuters Brasil**, 20 dez. 2013. Disponível em: <<http://br.reuters.com/article/domesticNews/idBRSP9BJ07Y20131220>>

WIRETAPPED: Israel Eavesdropped on John Kerry in Mideast Talks. **Der Spiegel Online**, 03 ago. 2014. Disponível em: <<http://www.spiegel.de/international/world/israel-intelligence-eavesdropped-on-phone-calls-by-john-kerry-a-984246.html>>

WISE, David. China's Spies are Catching Up. **The New York Times**, 10 dez. 2011. Disponível em: <<http://www.nytimes.com/2011/12/11/opinion/sunday/chinas-spies-are-catching-up.html>>

YANOFISKY, David; FERNHOLZ, Tim. The World above Us: This is every active satellite orbiting earth. **Quartz**. Disponível em: <<http://qz.com/296941/interactive-graphic-every-active-satellite-orbiting-earth/>>

YEGINSU, Ceylan. Paris Attacks: The Violence, its Victims and How the Investigation Unfolded. **The New York Times**, 16 nov. 2015. Disponível em: <<http://www.nytimes.com/live/paris-attacks-live-updates/turkey-warned-french-twice-about-attacker-official-says/>>

ANEXO 1

Key Judgments [from October 2002 NIE]

Iraq's Continuing Programs for Weapons of Mass Destruction

We judge that Iraq has continued its weapons of mass destruction (WMD) programs in defiance of UN resolutions and restrictions. Baghdad has chemical and biological weapons as well as missiles with ranges in excess of UN restrictions; if left unchecked, it probably will have a nuclear weapon during this decade. (See INR alternative view at the end of these Key Judgments.)

We judge that we are seeing only a portion of Iraq's WMD efforts, owing to Baghdad's vigorous denial and deception efforts. Revelations after the Gulf war starkly demonstrate the extensive efforts undertaken by Iraq to deny information. We lack specific information on many key aspects of Iraq's WMD programs.

Since inspections ended in 1998, Iraq has maintained its chemical weapons effort, energized its missile program, and invested more heavily in biological weapons; in the view of most agencies, Baghdad is reconstituting its nuclear weapons program.

- **Iraq's growing ability to sell oil illicitly increases Baghdad's capabilities to finance WMD programs; annual earnings in cash and goods have more than quadrupled, from \$580 million in 1998 to about \$3 billion this year.**
- **Iraq has largely rebuilt missile and biological weapons facilities damaged during Operation Desert Fox and has expanded its chemical and biological infrastructure under the cover of civilian production.**
- **Baghdad has exceeded UN range limits of 150 km with its ballistic missiles and is working with unmanned aerial vehicles (UAVs), which allow for a more lethal means to deliver biological and, less likely, chemical warfare agents.**
- **Although we assess that Saddam does not yet have nuclear weapons or sufficient material to make any, he remains intent on acquiring them. Most agencies assess that Baghdad started reconstituting its nuclear program about the time that UNSCOM inspectors departed—December 1998.**

How quickly Iraq will obtain its first nuclear weapon depends on when it acquires sufficient weapons-grade fissile material.

- **If Baghdad acquires sufficient fissile material from abroad it could make a nuclear weapon within several months to a year.**

- Without such material from abroad, Iraq probably would not be able to make a weapon until 2007 to 2009, owing to inexperience in building and operating centrifuge facilities to produce highly enriched uranium and challenges in procuring the necessary equipment and expertise.
 - Most agencies believe that Saddam's personal interest in and Iraq's aggressive attempts to obtain high-strength aluminum tubes for centrifuge rotors—as well as Iraq's attempts to acquire magnets, high-speed balancing machines, and machine tools—provide compelling evidence that Saddam is reconstituting a uranium enrichment effort for Baghdad's nuclear weapons program. (DOE agrees that reconstitution of the nuclear program is underway but assesses that the tubes probably are not part of the program.)
 - Iraq's efforts to re-establish and enhance its cadre of weapons personnel as well as activities at several suspect nuclear sites further indicate that reconstitution is underway.
 - All agencies agree that about 25,000 centrifuges based on tubes of the size Iraq is trying to acquire would be capable of producing approximately two weapons' worth of highly enriched uranium per year.
- In a much less likely scenario, Baghdad could make enough fissile material for a nuclear weapon by 2005 to 2007 if it obtains suitable centrifuge tubes this year and has all the other materials and technological expertise necessary to build production-scale uranium enrichment facilities.

We assess that Baghdad has begun renewed production of mustard, sarin, GF (cyclosarin), and VX; its capability probably is more limited now than it was at the time of the Gulf war, although VX production and agent storage life probably have been improved.

- An array of clandestine reporting reveals that Baghdad has procured covertly the types and quantities of chemicals and equipment sufficient to allow limited CW agent production hidden within Iraq's legitimate chemical industry.
- Although we have little specific information on Iraq's CW stockpile, Saddam probably has stocked at least 100 metric tons (MT) and possibly as much as 500 MT of CW agents—much of it added in the last year.
- The Iraqis have experience in manufacturing CW bombs, artillery rockets, and projectiles. We assess that they possess CW bulk fills for SRBM warheads, including for a limited number of covertly stored Scuds, possibly a few with extended ranges.

We judge that all key aspects—R&D, production, and weaponization—of Iraq's offensive BW program are active and that most elements are larger and more advanced than they were before the Gulf war.

- We judge Iraq has some lethal and incapacitating BW agents and is capable of quickly producing and weaponizing a variety of such agents, including anthrax, for delivery by bombs, missiles, aerial sprayers, and covert operatives.

- Chances are even that smallpox is part of Iraq's offensive BW program.
- Baghdad probably has developed genetically engineered BW agents.
- Baghdad has established a large-scale, redundant, and concealed BW agent production capability.
 - Baghdad has mobile facilities for producing bacterial and toxin BW agents; these facilities can evade detection and are highly survivable. Within three to six months* these units probably could produce an amount of agent equal to the total that Iraq produced in the years prior to the Gulf war.

Iraq maintains a small missile force and several development programs, including for a UAV probably intended to deliver biological warfare agent.

- Gaps in Iraqi accounting to UNSCOM suggest that Saddam retains a covert force of up to a few dozen Scud-variant SRBMs with ranges of 650 to 900 km.
- Iraq is deploying its new al-Samoud and Ababil-100 SRBMs, which are capable of flying beyond the UN-authorized 150-km range limit; Iraq has tested an al-Samoud variant beyond 150 km—perhaps as far as 300 km.
- Baghdad's UAVs could threaten Iraq's neighbors, US forces in the Persian Gulf, *and if brought close to, or into, the United States, the US Homeland.*
 - An Iraqi UAV procurement network attempted to procure commercially available route planning software and an associated topographic database that would be able to support targeting of the United States, according to analysis of special intelligence.
 - The Director, Intelligence, Surveillance, and Reconnaissance, US Air Force, does not agree that Iraq is developing UAVs *primarily* intended to be delivery platforms for chemical and biological warfare (CBW) agents. The small size of Iraq's new UAV strongly suggests a primary role of reconnaissance, although CBW delivery is an inherent capability.
- Iraq is developing medium-range ballistic missile capabilities, largely through foreign assistance in building specialized facilities, including a test stand for engines more powerful than those in its current missile force.

We have low confidence in our ability to assess when Saddam would use WMD.

- Saddam could decide to use chemical and biological warfare (CBW) preemptively against US forces, friends, and allies in the region in an attempt to disrupt US war preparations and undermine the political will of the Coalition.

*[Corrected per Errata sheet issued in October 2002]

- Saddam might use CBW after an initial advance into Iraqi territory, but early use of WMD could foreclose diplomatic options for stalling the US advance.
- He probably would use CBW when he perceived he irretrievably had lost control of the military and security situation, but we are unlikely to know when Saddam reaches that point.
- We judge that Saddam would be more likely to use chemical weapons than biological weapons on the battlefield.
- Saddam historically has maintained tight control over the use of WMD; however, he probably has provided contingency instructions to his commanders to use CBW in specific circumstances.

Baghdad for now appears to be drawing a line short of conducting terrorist attacks with conventional or CBW against the United States, fearing that exposure of Iraqi involvement would provide Washington a stronger cause for making war.

Iraq probably would attempt clandestine attacks against the US Homeland if Baghdad feared an attack that threatened the survival of the regime were imminent or unavoidable, or possibly for revenge. Such attacks—more likely with biological than chemical agents—probably would be carried out by special forces or intelligence operatives.

- The Iraqi Intelligence Service (IIS) probably has been directed to conduct clandestine attacks against US and Allied interests in the Middle East in the event the United States takes action against Iraq. The IIS probably would be the primary means by which Iraq would attempt to conduct any CBW attacks on the US Homeland, although we have no specific intelligence information that Saddam's regime has directed attacks against US territory.

Saddam, if sufficiently desperate, might decide that only an organization such as al-Qa'ida—with worldwide reach and extensive terrorist infrastructure, and already engaged in a life-or-death struggle against the United States—could perpetrate the type of terrorist attack that he would hope to conduct.

- In such circumstances, he might decide that the extreme step of assisting the Islamist terrorists in conducting a CBW attack against the United States would be his last chance to exact vengeance by taking a large number of victims with him.

State/INR Alternative View of Iraq's Nuclear Program

The Assistant Secretary of State for Intelligence and Research (INR) believes that Saddam continues to want nuclear weapons and that available evidence indicates that Baghdad is pursuing at least a limited effort to maintain and acquire nuclear weapon-related capabilities. The activities we have detected do not, however, add up to a compelling case that Iraq is currently pursuing what INR would consider to be an integrated and comprehensive approach to

(continued on next page...)

(continued...) State/INR Alternative View

acquire nuclear weapons. Iraq may be doing so, but INR considers the available evidence inadequate to support such a judgment. Lacking persuasive evidence that Baghdad has launched a coherent effort to reconstitute its nuclear weapons program, INR is unwilling to speculate that such an effort began soon after the departure of UN inspectors or to project a timeline for the completion of activities it does not now see happening. As a result, INR is unable to predict when Iraq could acquire a nuclear device or weapon.

In INR's view Iraq's efforts to acquire aluminum tubes is central to the argument that Baghdad is reconstituting its nuclear weapons program, but INR is not persuaded that the tubes in question are intended for use as centrifuge rotors. INR accepts the judgment of technical experts at the U.S. Department of Energy (DOE) who have concluded that the tubes Iraq seeks to acquire are poorly suited for use in gas centrifuges to be used for uranium enrichment and finds unpersuasive the arguments advanced by others to make the case that they are intended for that purpose. INR considers it far more likely that the tubes are intended for another purpose, most likely the production of artillery rockets. The very large quantities being sought, the way the tubes were tested by the Iraqis, and the atypical lack of attention to operational security in the procurement efforts are among the factors, in addition to the DOE assessment, that lead INR to conclude that the tubes are not intended for use in Iraq's nuclear weapon program.

Confidence Levels for Selected Key Judgments in This Estimate

High Confidence:

- Iraq is continuing, and in some areas expanding, its chemical, biological, nuclear and missile programs contrary to UN resolutions.
- We are not detecting portions of these weapons programs.
- Iraq possesses proscribed chemical and biological weapons and missiles.
- Iraq could make a nuclear weapon in months to a year once it acquires sufficient weapons-grade fissile material.

Moderate Confidence:

- Iraq does not yet have a nuclear weapon or sufficient material to make one but is likely to have a weapon by 2007 to 2009. (See INR alternative view, page 84).

Low Confidence:

- When Saddam would use weapons of mass destruction.
- Whether Saddam would engage in clandestine attacks against the US Homeland.
- Whether in desperation Saddam would share chemical or biological weapons with al-Qa'ida.

Uranium Acquisition. Iraq retains approximately two-and-a-half tons of 2.5 percent enriched uranium oxide, which the IAEA permits. This low-enriched material could be used as feed material to produce enough HEU for about two nuclear weapons. The use of enriched feed material also would reduce the initial number of centrifuges that Baghdad would need by about half. Iraq could divert this material—the IAEA inspects it only once a year—and enrich it to weapons

grade before a subsequent inspection discovered it was missing. The IAEA last inspected this material in late January 2002.

Iraq has about 550 metric tons of yellowcake¹ and low-enriched uranium at Tuwaitha, which is inspected annually by the IAEA. Iraq also began vigorously trying to procure uranium ore and yellowcake; acquiring either would shorten the time Baghdad needs to produce nuclear weapons.

- A foreign government service reported that as of early 2001, Niger planned to send several tons of "pure uranium" (probably yellowcake) to Iraq. As of early 2001, Niger and Iraq reportedly were still working out arrangements for this deal, which could be for up to 500 tons of yellowcake. We do not know the status of this arrangement.
- Reports indicate Iraq also has sought uranium ore from Somalia and possibly the Democratic Republic of the Congo.

We cannot confirm whether Iraq succeeded in acquiring uranium ore and/or yellowcake from these sources. Reports suggest Iraq is shifting from domestic mining and milling of uranium to foreign acquisition. Iraq possesses significant phosphate deposits, from which uranium had been chemically extracted before Operation Desert Storm. Intelligence information on whether nuclear-related phosphate mining and/or processing has been reestablished is inconclusive, however.

¹ A refined form of natural uranium.

Annex A

Iraq's Attempts to Acquire Aluminum Tubes

[This excerpt from a longer view includes INR's position on the African uranium issue]

INR's Alternative View: Iraq's Attempts to Acquire Aluminum Tubes

Some of the specialized but dual-use items being sought are, by all indications, bound for Iraq's missile program. Other cases are ambiguous, such as that of a planned magnet-production line whose suitability for centrifuge operations remains unknown. Some efforts involve non-controlled industrial material and equipment—including a variety of machine tools—and are troubling because they would help establish the infrastructure for a renewed nuclear program. But such efforts (which began well before the inspectors departed) are not clearly linked to a nuclear end-use. Finally, the claims of Iraqi pursuit of natural uranium in Africa are, in INR's assessment, highly dubious.

ANEXO 2

Bin Ladin Determined To Strike in US



Clandestine, foreign government, and media reports indicate Bin Ladin since 1997 has wanted to conduct terrorist attacks in the US. Bin Ladin implied in US television interviews in 1997 and 1998 that his followers would follow the example of World Trade Center bomber Ramzi Yousef and "bring the fighting to America."

After US missile strikes on his base in Afghanistan in 1998, Bin Ladin told followers he wanted to retaliate in Washington, according to a [REDACTED] service.

An Egyptian Islamic Jihad (EIJ) operative told an [REDACTED] service at the same time that Bin Ladin was planning to exploit the operative's access to the US to mount a terrorist strike.

The millennium plotting in Canada in 1999 may have been part of Bin Ladin's first serious attempt to implement a terrorist strike in the US. Convicted plotter Ahmed Ressaam has told the FBI that he conceived the idea to attack Los Angeles International Airport himself, but that Bin Ladin lieutenant Abu Zubaydah encouraged him and helped facilitate the operation. Ressaam also said that in 1998 Abu Zubaydah was planning his own US attack.

Ressaam says Bin Ladin was aware of the Los Angeles operation.

Although Bin Ladin has not succeeded, his attacks against the US Embassies in Kenya and Tanzania in 1998 demonstrate that he prepares operations years in advance and is not deterred by setbacks. Bin Ladin associates surveilled our Embassies in Nairobi and Dar es Salaam as early as 1993, and some members of the Nairobi cell planning the bombings were arrested and deported in 1997.

Al-Qa'ida members—including some who are US citizens—have resided in or traveled to the US for years, and the group apparently maintains a support structure that could aid attacks. Two al-Qa'ida members found guilty in the conspiracy to bomb our Embassies in East Africa were US citizens, and a senior EIJ member lived in California in the mid-1990s.

A clandestine source said in 1998 that a Bin Ladin cell in New York was recruiting Muslim-American youth for attacks.

We have not been able to corroborate some of the more sensational threat reporting, such as that from a [REDACTED] service in 1998 saying that Bin Ladin wanted to hijack a US aircraft to gain the release of "Blind Shaykh" 'Umar 'Abd al-Rahman and other US-held extremists.

continued

- Nevertheless, FBI information since that time indicates patterns of suspicious activity in this country consistent with preparations for hijackings or other types of attacks, including recent surveillance of federal buildings in New York.

The FBI is conducting approximately 70 full field investigations throughout the US that it considers Bin Ladin-related. CIA and the FBI are investigating a call to our Embassy in the UAE in May saying that a group of Bin Ladin supporters was in the US planning attacks with explosives.

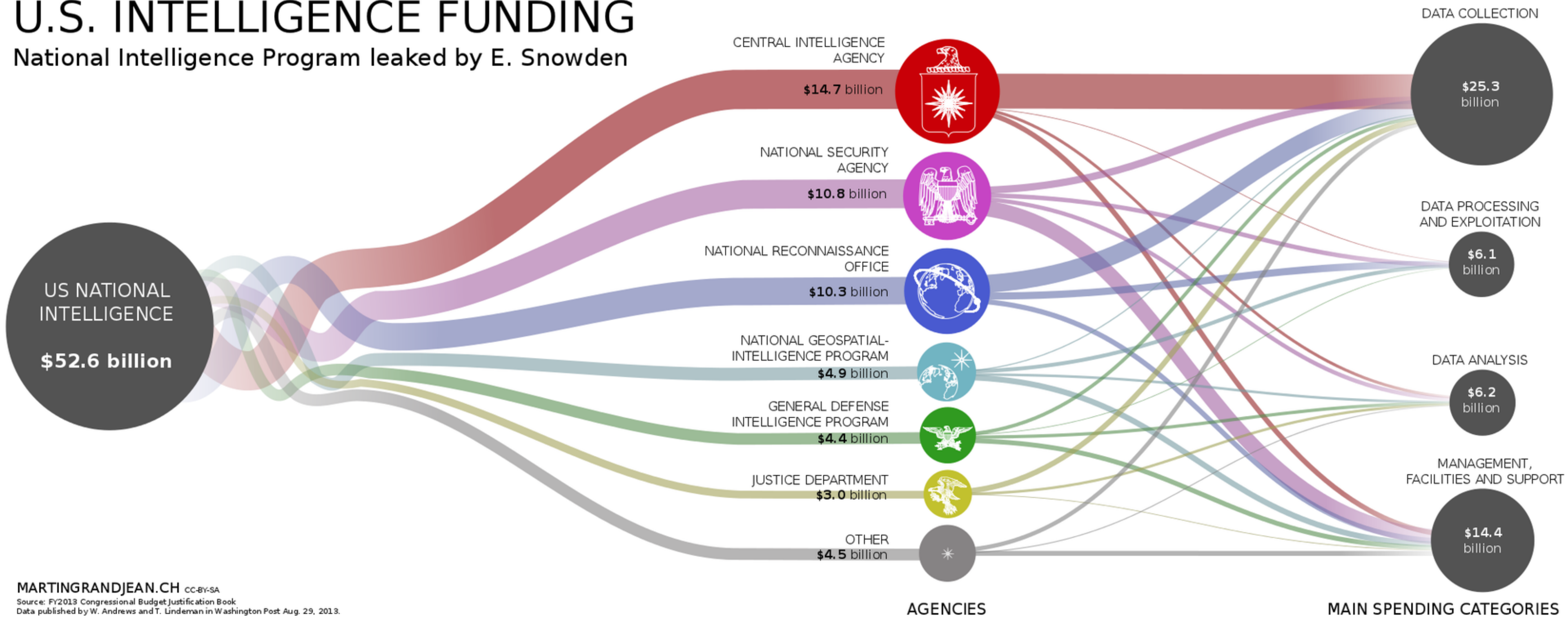
For the President Only
6 August 2001

 Declassified and Approved
for Release, 10 April 2004

ANEXO 3

U.S. INTELLIGENCE FUNDING

National Intelligence Program leaked by E. Snowden



ANEXO 4

TOP SECRET//SI//NOFORN

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13 - 8 0

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

TOP SECRET//SI//NOFORN

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries.

Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c)

TOP SECRET//SI//NOFORN

shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

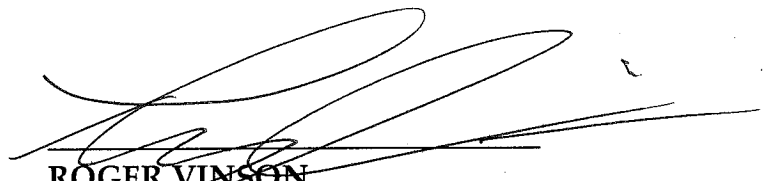
-- Remainder of page intentionally left blank. --

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

This authorization requiring the production of certain call detail records or
"telephony metadata" created by Verizon expires on the 19th day of July, 2013, at
5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time


ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

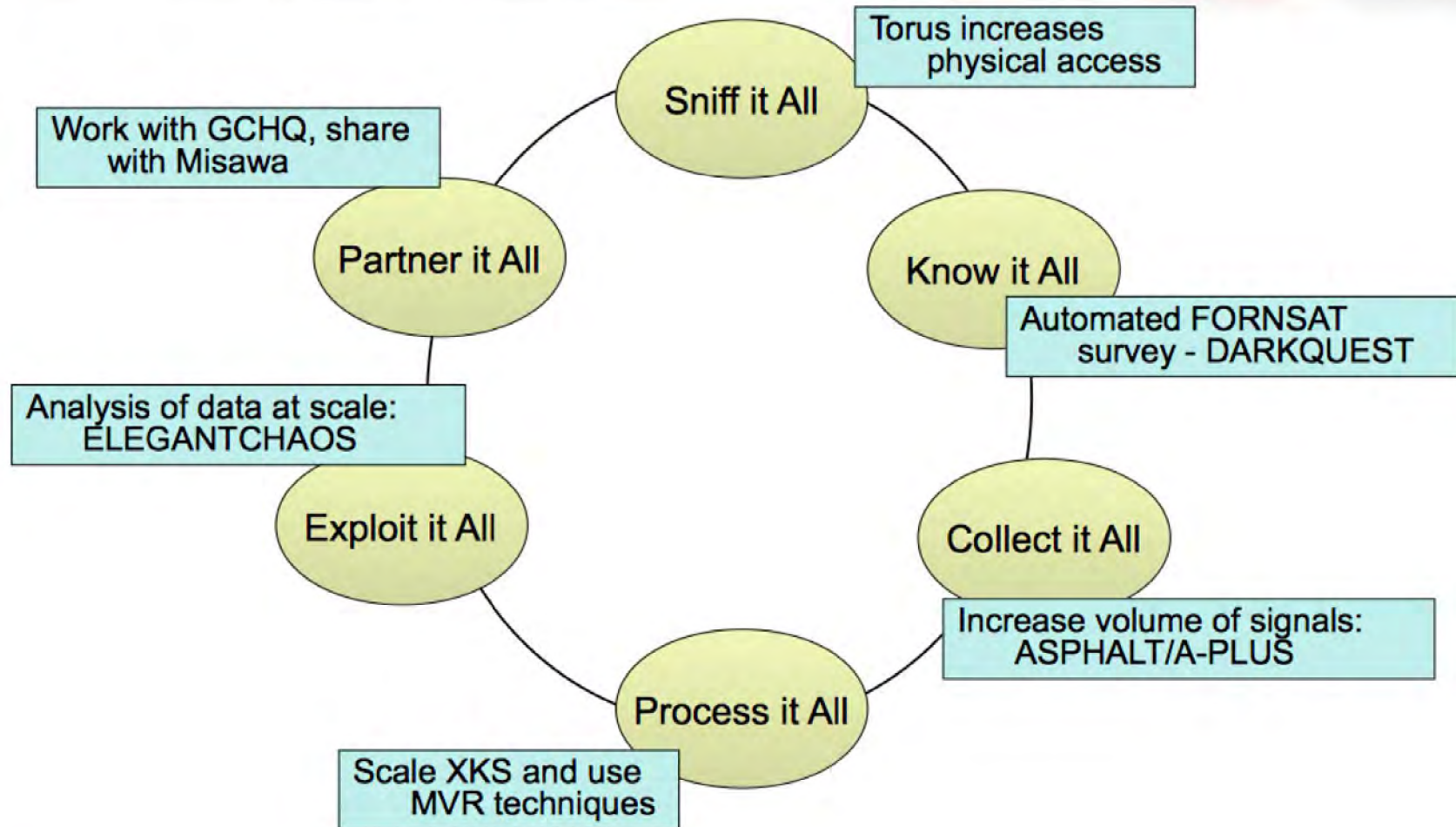
I, Beverly C. Queen, Chief Deputy
Clerk, FISC, certify that this document
is a true and correct copy of the
original. 

TOP SECRET//SI//NOFORN

ANEXO 5

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

New Collection Posture



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

ANEXO 6

TOP SECRET//COMINT//NOFORN

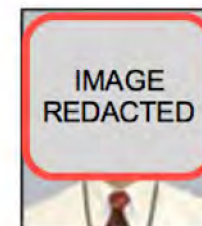
June 2010



(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

By: (U//FOUO) NAME REDACTED, Chief, Access and Target Development (S3261)

(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away... In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.



(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

(TS//SI//NF) In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure. This call back provided us access to further exploit the device and survey the network.

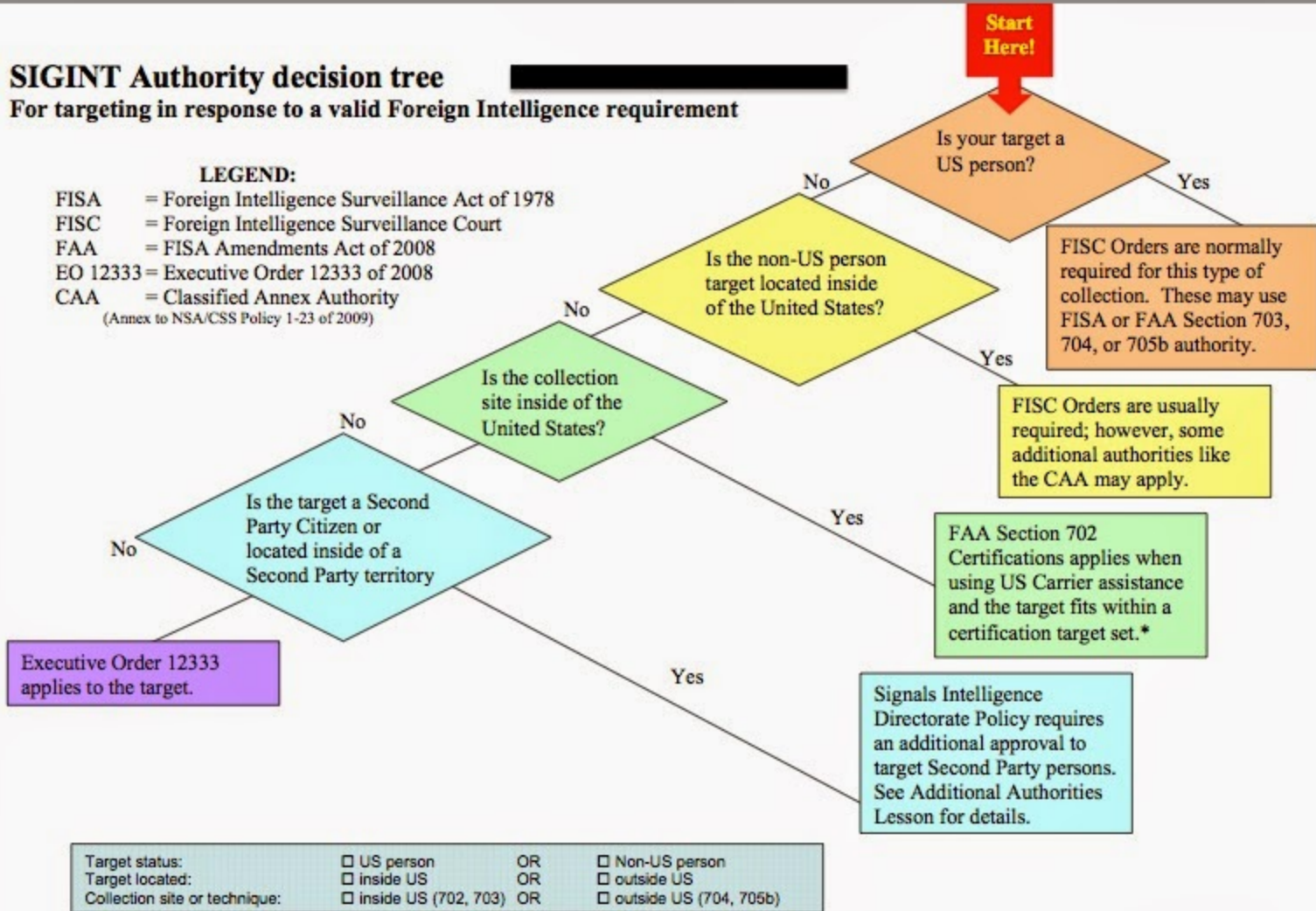
ANEXO 7

SIGINT Authority decision tree

For targeting in response to a valid Foreign Intelligence requirement

LEGEND:

FISA = Foreign Intelligence Surveillance Act of 1978
FISC = Foreign Intelligence Surveillance Court
FAA = FISA Amendments Act of 2008
EO 12333 = Executive Order 12333 of 2008
CAA = Classified Annex Authority
(Annex to NSA/CSS Policy 1-23 of 2009)



* Some FORNSAT and SCS sites may be physically located inside of the United States however; they are treated like foreign Conventional Collection sites

ANEXO 8

BACKGROUND (U)

(TS//SI//REL TO USA, FVEY) A previous SIGINT assessment report on radicalization indicated that radicalizers appear to be particularly vulnerable in the area of authority when their private and public behaviors are not consistent. (A) Some of the vulnerabilities, if exposed, would likely call into question a radicalizer's devotion to the jihadist cause, leading to the degradation or loss of his authority. Examples of some of these vulnerabilities include:

- Viewing sexually explicit material online or using sexually explicit persuasive language when communicating with inexperienced young girls;
- Using a portion of the donations they are receiving from the susceptible pool to defray their own personal expenses;
- Charging an exorbitant amount of money for their speaking fees and being singularly attracted by opportunities to increase their stature; or
- Being known to base their public messaging on questionable sources or using language that is contradictory in nature, leaving them open to credibility challenges.

(TS//SI//REL TO USA, FVEY) Issues of trust and reputation are important when considering the validity and appeal of the message. It stands to reason that exploiting vulnerabilities of character, credibility, or both, of the radicalizer and his message could be enhanced by an understanding of the vehicles he uses to disseminate his message to the susceptible pool of people and where he is vulnerable in terms of access.

ANEXO 9



TOP SECRET//SI//REL TO USA, FVEY



Private Networks are Important

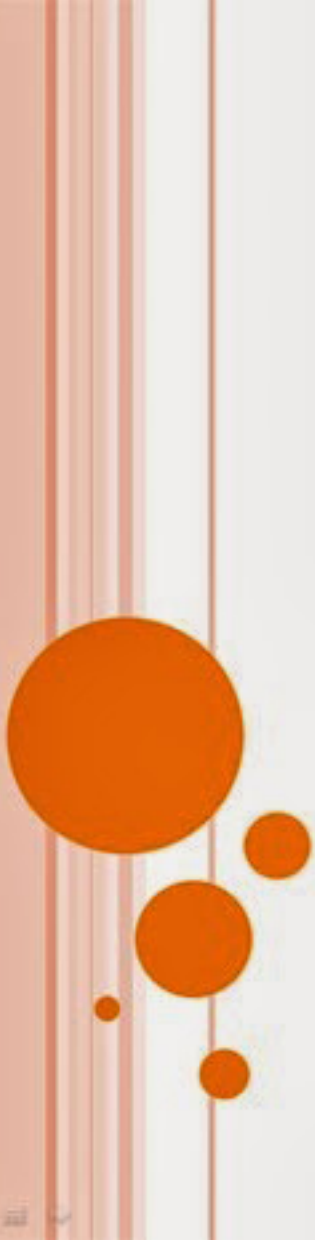
- Many targets use private networks.

Google infrastructure	SWIFT Network
REDACTED	REDACTED
REDACTED	Gazprom
Aeroflot	REDACTED
French MFA	REDACTED
Warid Telecom	Petrobras
REDACTED	REDACTED

- Evidence in Survey: 30%-40% of traffic in BLACKPEARL has at least one endpoint private.

TOP SECRET//SI//REL TO USA, FVEY

ANEXO 10



**AND THEY SAID TO THE TITANS:
« WATCH OUT OLYMPIANS IN
THE HOUSE! »**

**CSEC – Advanced Network Tradecraft
SD Conference June 2012**

Overall Classification: TOP SECRET//SI

OLYMPIA & THE CASE STUDY



OLYMPIA

CSEC's Network Knowledge Engine

Various data sources
Chained enrichments
Automated analysis

Brazilian Ministry of Mines and Energy (MME)

New target to develop
Limited access/target knowledge

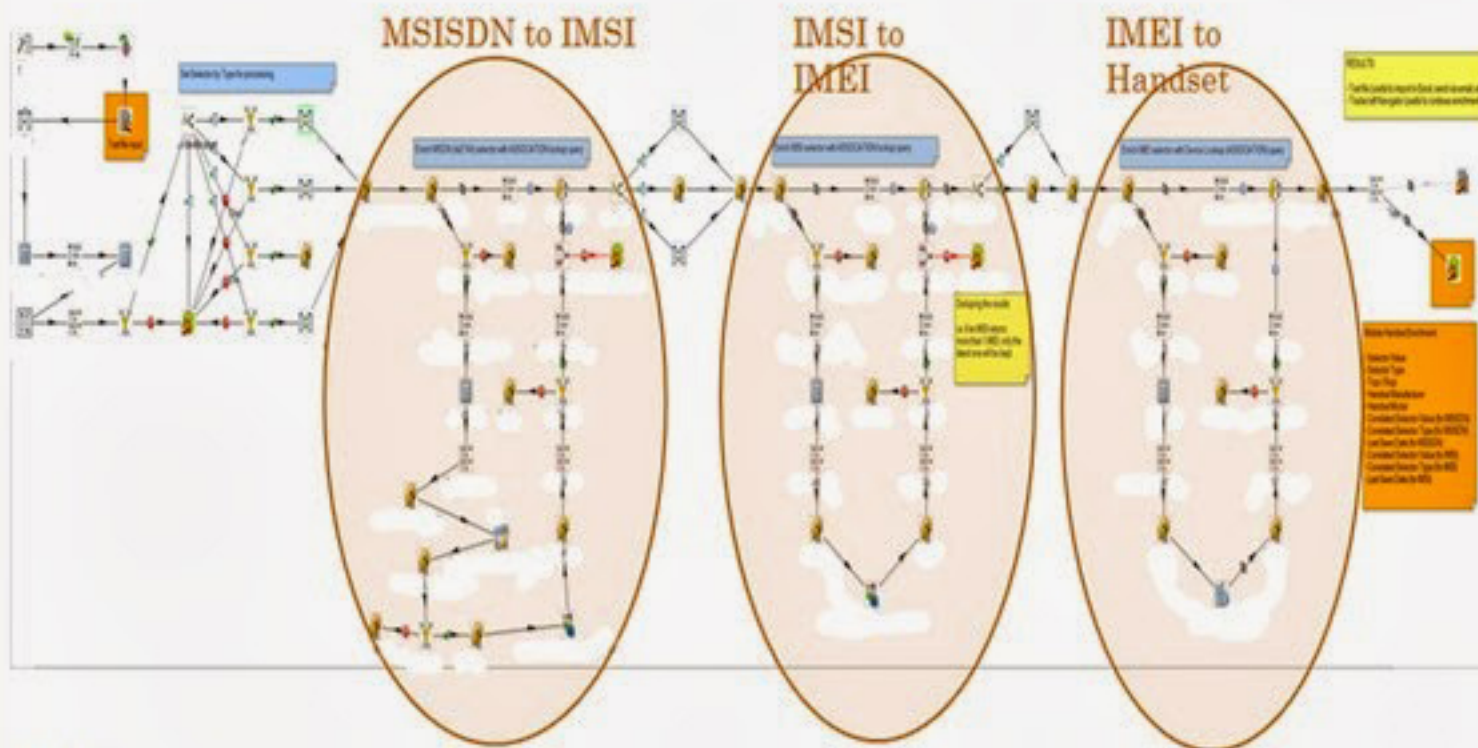


QUESTIONS

- How can I use the information available in SIGINT data sources to learn about the target?
- What can I find that would help me inform access development efforts?
- Can I automate the analytical process and/or re-use analytics designed for other purposes?



ANALYSIS- REVEAL TARGET'S HANDSETS

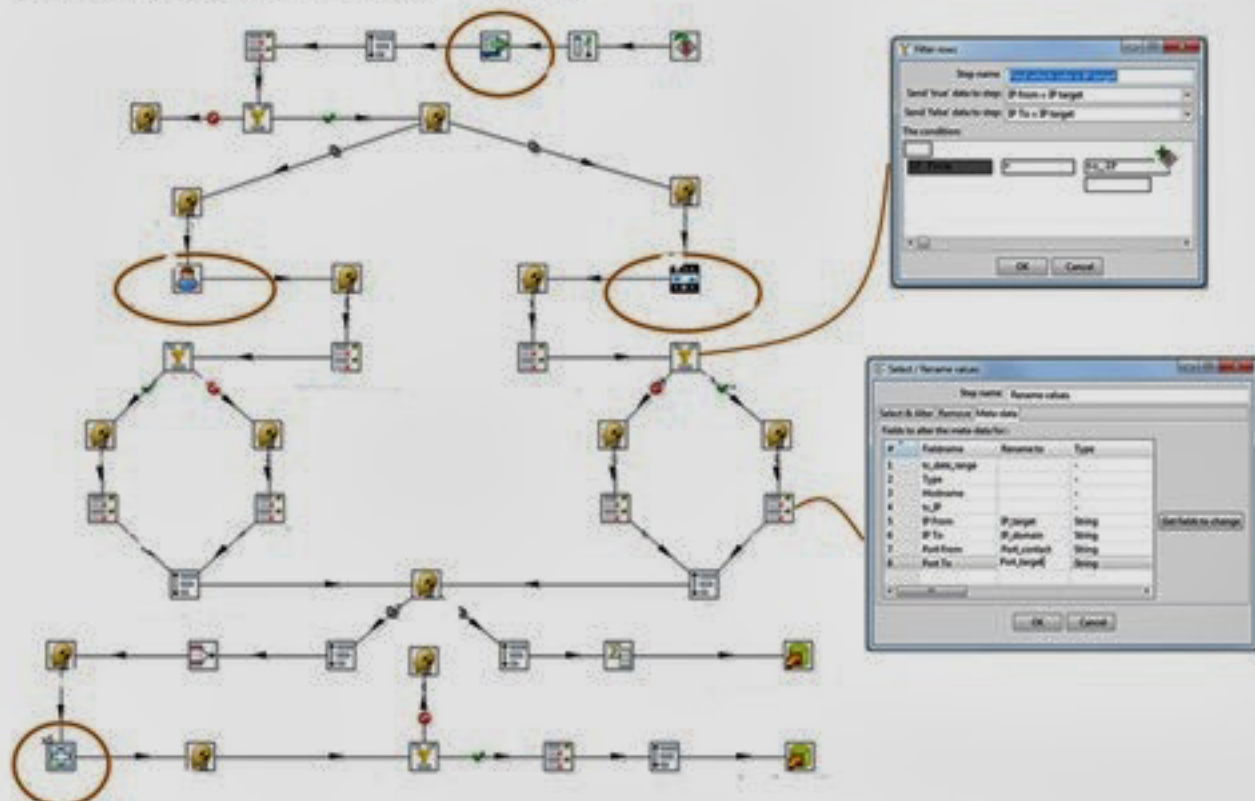


Output

Original Selector Value for MSISDN	Original Selector Type for MSISDN	IMSI Correlation	IMEI Correlation	Bands Supported for IMEI	Manufacturer for IMEI	Marketing Name for IMEI	TOPI
	ITU164			GSM 1800, GSM 1900, GSM 900, GSM850 (GSM800), WCDMA FDD	Nokia Corporation	3120c-1c	CSEC
	ITU164			GSM 1800, GSM 1900, GSM 900, GSM850 (GSM800), HSDPA, HSUPA	Motorola Mobility	Motorola MURQ7-3334413C11	CSEC

Nokia 3120c-1c
Motorola MURQ7

ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH



ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH

Hostname domain	IP in contact with domain	Owner of IP contact	Carrier of IP contact	ASN of IP contact	Country of IP contact
correo.mme.gov.br	196.200.330.214	br i net noc ip infrastructure	british telecommunications plc	5400 entrea	
correo.mme.gov.br	196.200.330.5	br i net noc ip infrastructure	british telecommunications plc	5400 entrea	
correo.mme.gov.br	207.45.217.30	tata communications	tata communications	6403 canada	
correo.mme.gov.br	213.119.60.87	jitc	jordan telecommunications com	9897 jordan	
correo.mme.gov.br	216.1.31.40	reassign to idc-dw-idc customer	cs loxinfo public company limited	9891 thailand	
correo.mme.gov.br	212.34.328.17	internal network	international data exchange llc	12024 jordan	
correo.mme.gov.br	188.245.245.222	pars online	parsonline	16022 iran	
correo.mme.gov.br	188.50.21.63	dsl home subscribers	saudinet	25029 saudi arabia	
correo.mme.gov.br	188.51.267.2	dsl home subscribers	saudinet	25029 saudi arabia	
correo.mme.gov.br	188.54.68.142	dsl home subscribers	saudinet	25029 saudi arabia	
correo.mme.gov.br	212.118.343.38	saudinet	saudi telecom compan saudinet	25029 saudi arabia	
correo.mme.gov.br	209.172.51.39	web dedicated hd	web technologies inc.	12613 canada	
correo.mme.gov.br	209.172.51.171	web dedicated hd	web technologies inc.	12613 canada	
correo.mme.gov.br	212.307.330.105	middle east internet company llc	cyberia ryadh	34097 saudi arabia	
www.mme.gov.br	213.236.12.31	adl service	shura net	41176 saudi arabia	

Hostname starting domain
 IP starting domain
 IP in contact with starting domain
 Port used by starting domain
 Port used by IP contact

Owner of IP contact
 Carrier of IP contact
 ASN of IP contact
 Country of IP contact
 IP range for IP contact



MOVING FORWARD

- I have identified MX servers which have been targeted to passive collection by the Intel analysts, who are assessing the value, provenance, etc. of the traffic generated by the mail servers.
- I am working with TAO to further examine the possibility for a Man on the Side operation.
- Based on the network information gathered, the NAC has started a BPoA analysis on the MME.

ANEXO 11

BOUNDLESSINFORMANT

[Map View](#) [Org View](#)
☒ AGGREGATE ☐ DNI ☐ DNR

 [Country View](#)

OVERVIEW

(LAST 30 DAYS)

TOTAL DNI

97,111,188,358

TOTAL DNR

124,808,692,959

SIGADS

504

CASE NOTATIONS

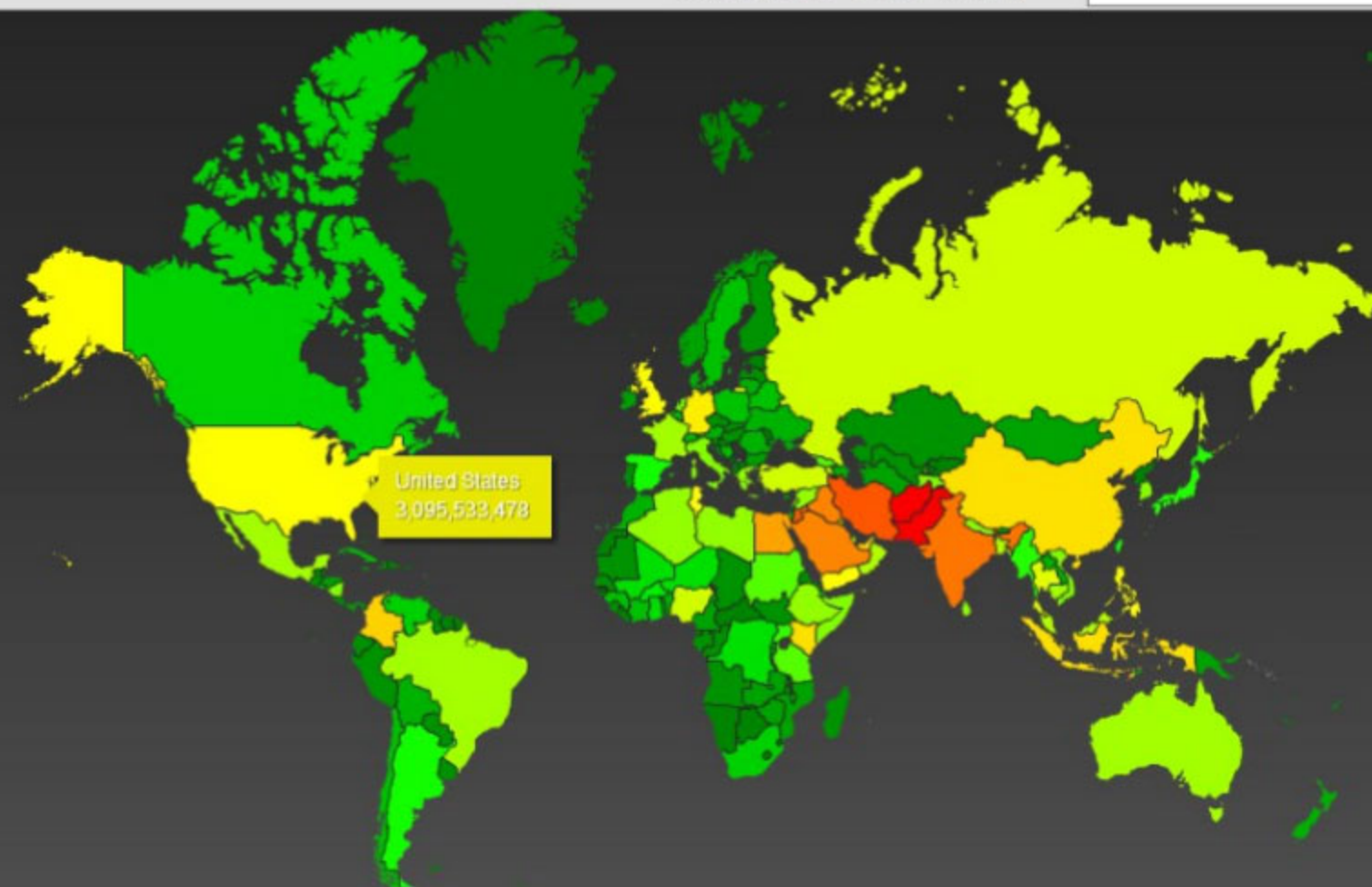
27,798

PROCESSING SYSTEMS

2,431

Global

map by amMap.com


Top 5 Countries (Last 30 Days from today)


Country	DNI	DNR
Pakistan	13,516,527,385	13,759,417,233
Afghanistan	2,316,972,214	21,977,001,389
Iran, Islamic Republic of	14,101,066,499	1,733,419,401
Jordan	12,729,653,438	1,644,602,031
India	6,333,878,580	6,283,036,977

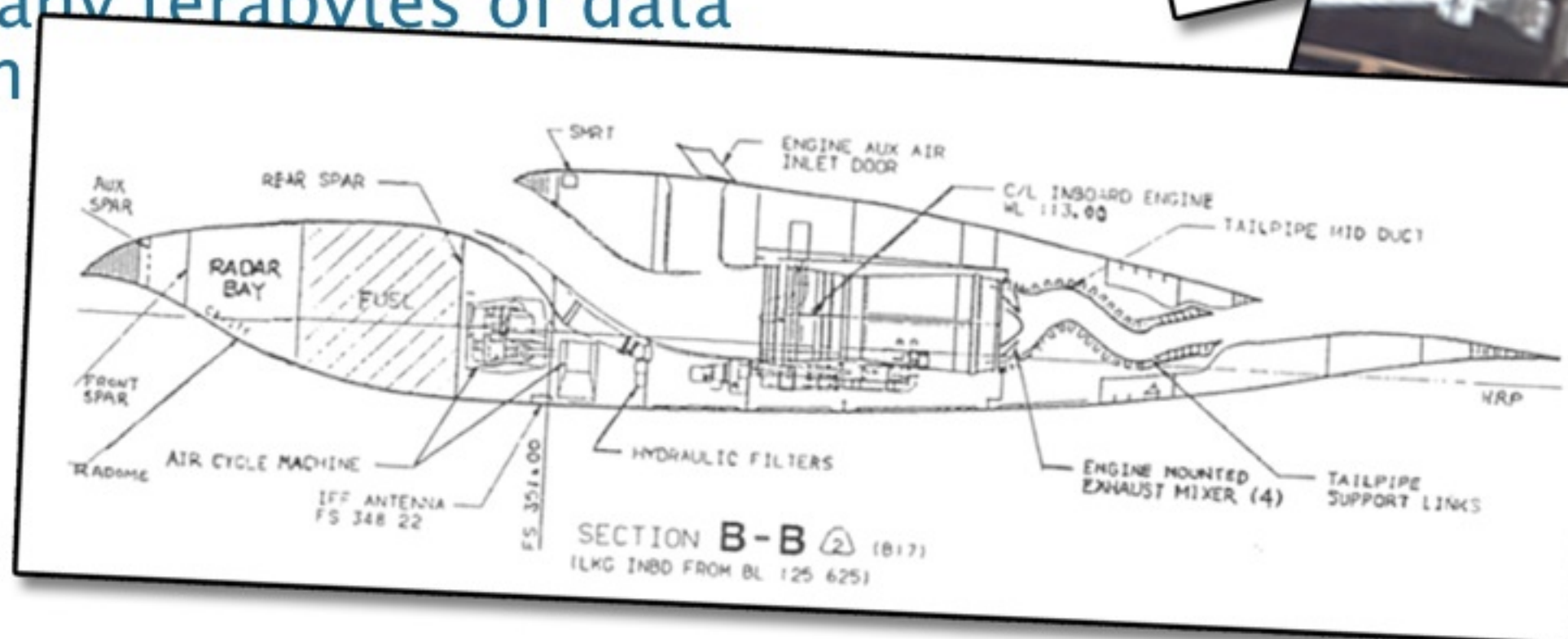
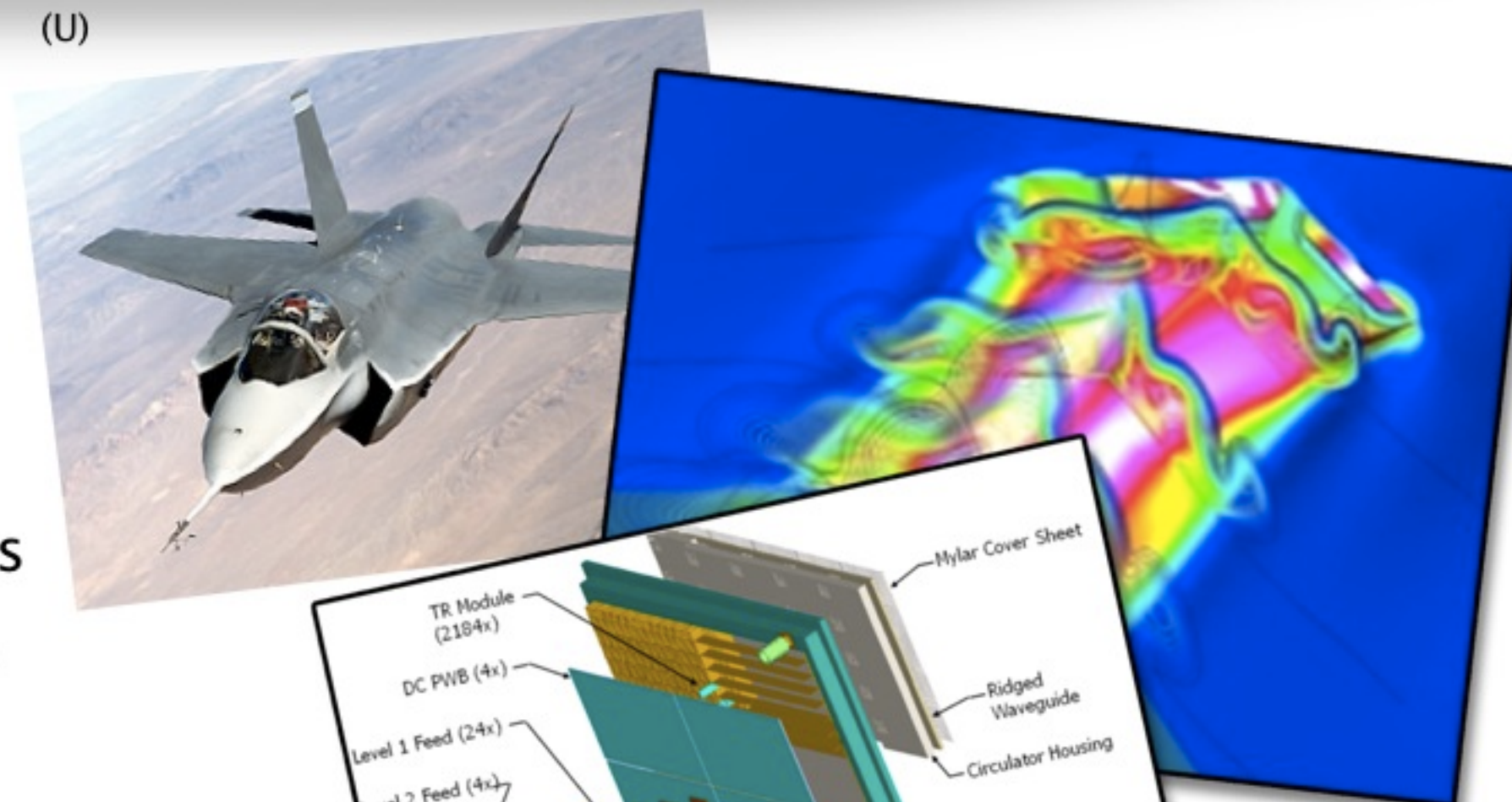
ANEXO 12

(S//REL) Chinese Exfiltrate Sensitive Military Technology



- (U) Acquired radar design
 - (U) Numbers and types of modules
- (U) Detailed engine schematics
 - (U) Methods for cooling gases
 - (U) Leading and trailing edge treatments
 - (U) Aft deck heating contour maps
- (U) Many terabytes of data stolen

(U)



(U)



(S//REL) BYZANTINE HADES Causes Serious Damage to DoD Interests

(S//REL)

(S//REL) Resources Expended Towards

Response to Attacks

(S//REL) Personnel, Network, Logistics Data, Compromises

- At least +30,000 Incidents/+500 Significant Intrusions in DoD Systems
- At least +1600 Network Computers Penetrated
- At least 600,00 User Accounts Compromised
- +\$100 Million to Assess Damage, Rebuild Networks

- USPACOM: Air Refueling Schedules (CORONET)
- USTRANSCOM: Single Mobility System (SMS)
- U.S. Air Force: 33,000 General/Field Grade Officer Records
- Navy: Over 300,00 User ID/Passwords Compromised
- Navy: Missile Navigation and Tracking Systems
- Navy: Nuclear Submarine/Anti-Air Missile Designs

(S//REL) Science & Technology Export Controlled Data

- International Traffic and Arms Restrictions (ITAR) Data
- Contractor Research & Development
- Defense Industrial Espionage
 - B2, F-22, F-35, Space-Based Laser, Others

(S//REL)

**(S//REL) Estimated Equivalent of Five Libraries of Congress
(50 Terabytes)**

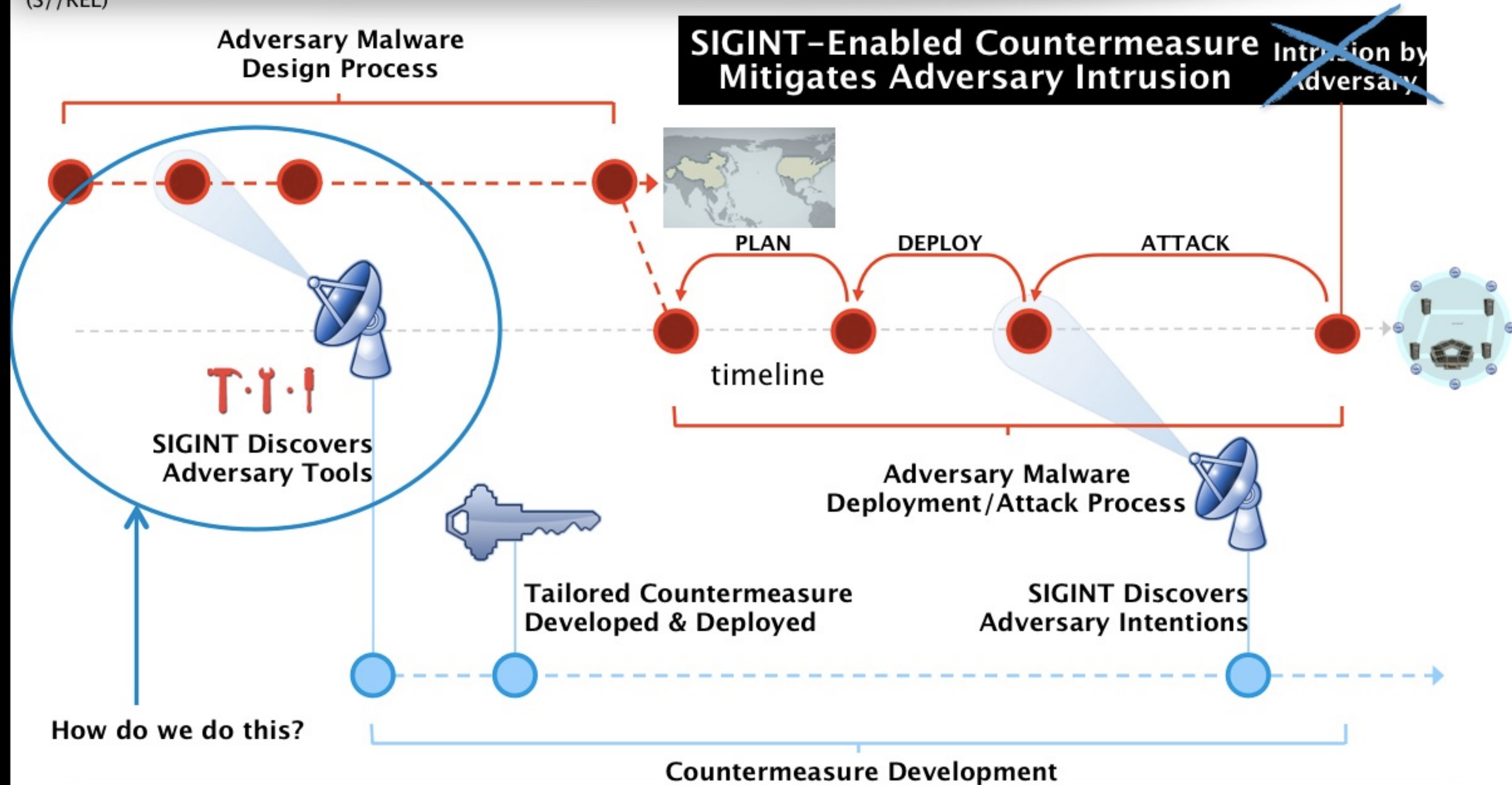


(U) Cyber Attack and Mitigation Timelines

TOP SECRET//COMINT//REL USA, FVEY



(S//REL)



(S//REL) How do we use SIGINT to discover Malware during the design process?

(S//REL)

ANEXO 13

**(TS//SI//REL) Intelligently filtering your data:
Brazil and Mexico case studies**

SATC

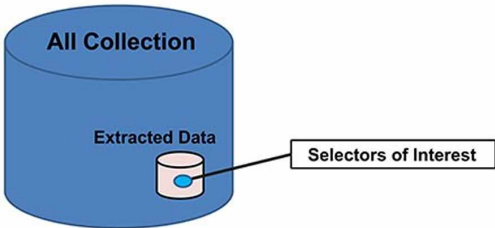
(U) Classification

This presentation is classified

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) The benefits

- (S//REL) Extracts from the full collection of data the activity most relevant to the selectors of interest

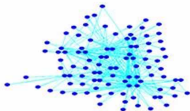


(U) The benefits

- (S//REL) Allows the analyst to implement analytics that
 - Are customized to their needs on a target-by-target basis
 - Could not or should not be run against all collection
 - Might find a needle in a haystack in an repeatable and efficient way

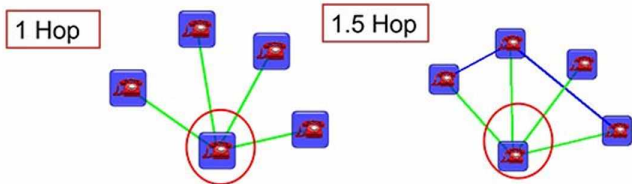
(U) Contact Graphs

- (U) A **graph** is a set of objects (nodes, vertices) connected by links (edges).
- (U) Graphs are a useful way of visualizing and analyzing the structure of communication networks



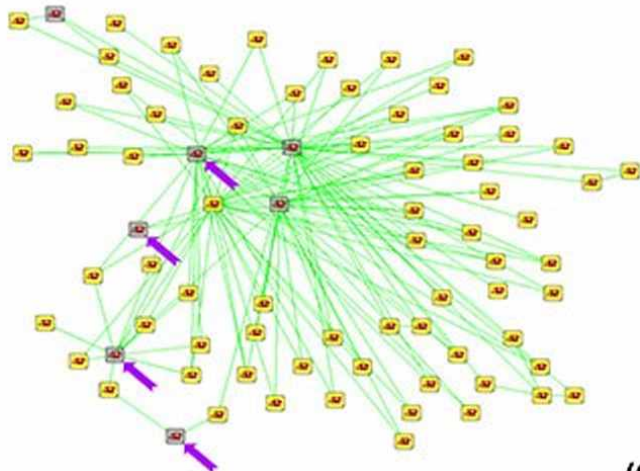
(U) Hops

- (U) We may build a 1-hop graph by selecting all vertices connected to a root node
- (U) A 1.5-hop graph contains all vertices connected to a root node and all connections between those vertices



(U) applications in target development

(C/REL)



(C/REL)

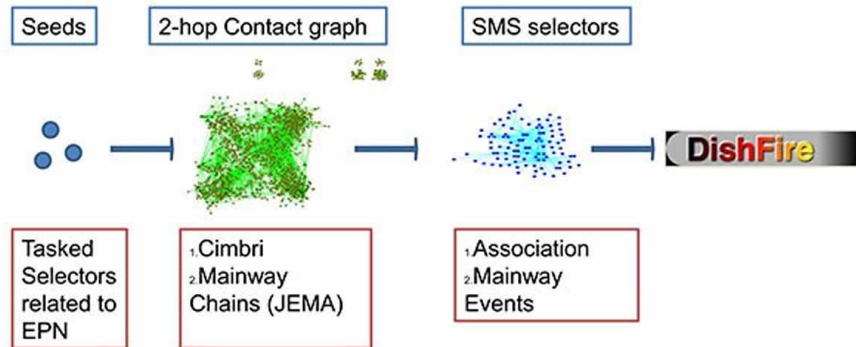
(U//FOUO) S2C41 surge effort

(TS//SI//REL) NSA's Mexico Leadership Team (S2C41) conducted a two-week target development surge effort against one of Mexico's leading presidential candidates, Enrique Pena Nieto, and nine of his close associates. Nieto is considered by most political pundits to be the likely winner of the 2012 Mexican presidential elections which are to be held in July 2012. SATC leveraged graph analysis in the development surge's target development effort.



(U) One-Time Work

(TS//SI//REL)



(TS//SI//REL)

(U) Results

▣(S//SI//REL)85489 Text messages

Interesting Messages

[REDACTED] Me dice Jorge Corona Srio de EPN que el escucho que BPA se iba a con Moreira no es asi? Y pues va soka salvo que le digas a alguien,,Asoc ID not requested,not requested,not requested,, [REDACTED]

Nieto

[REDACTED], Mi Querido Alex el nuevo titular de Com. Social es Juan Ramon Flores su cel es [REDACTED] el ID [REDACTED] Nuevo Srio. Part. Es Lic. Miguel Angel Gonzalez Cel [REDACTED] el Nuevo ID de JORGE CORONA es [REDACTED] un abrazo y seguimos en contacto avisame si llego el msj. por favor,,,,, [REDACTED]

(U//FOUO) S2C42 surge effort

(U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.



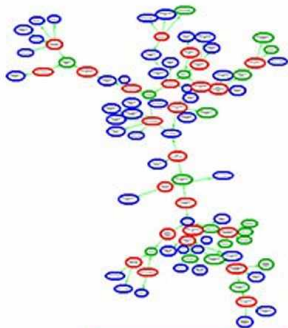
(U) One-Time Work

(TS//SI//REL)

Seeds



2-hop Contact graph



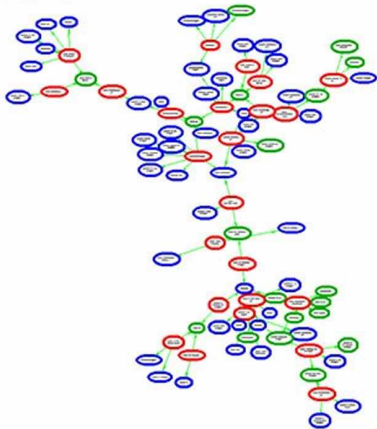
DNI
selectors

SCIMITAR

(TS//SI//REL)

(U//FOUO) S2C42 surge effort

(TS//SI//REL)



Discovered new selectors associated with high-value targets

(TS//SI//REL)

(U) Conclusion

- (S//REL) Contact graph-enhanced filtering is a simple yet effective technique, which may allow you to find previously unobtainable results and empower analytic discovery
- (TS//SI//REL) Teaming with S2C, SATC was able to successfully apply this technique against high-profile, OPSEC-savvy Brazilian and Mexican targets.



(U//FOUO) Geopolitical Trends for 2014-2019:

Identifying

Derived From NSA/CSSM 1-12

Dated: 20070108

Declassify On: 202870501

Challenges



0.0



U//FOUO



The Overall Classification Is:

TOP SECRET//SI//REL TO USA, FVEY

Geopolitical Trends: Global Drivers

(S//REL) Geopolitical Trend drivers:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- **Stressors to Regional Stability/Rise of New Actors.**

- Brazil and Turkey emerge on the global stage, Mexico is stressed and on our border, Arab Spring continues, the global "youth bulge" causes disaffection among youths who cannot find employment.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Geopolitical Trends: Key Challenges

(S//REL) Transnational Issues

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(S//REL) Nation-State Issues

[REDACTED]

[REDACTED]

[REDACTED]

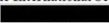
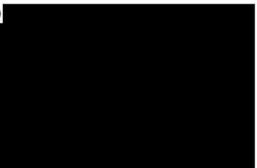
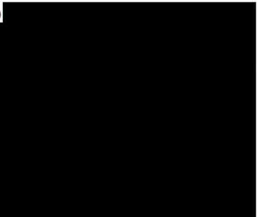
[REDACTED]

[REDACTED]

- Friends, Enemies, or Problems?
 - Brazil, Egypt, India, Iran, Mexico, Saudi Arabia, Somalia, Sudan, Turkey, Yemen, and others.

[REDACTED]

DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL		
Welcome! Friday, 09 Nov 2012		
• Web search • Agency-all Emails • SID-all Emails • NSA Rolodex • SCQAWK: The SID Mailbag • SIDtoday Blog • SIDtoday Series • SIGINT Worldwide VTC		
• SIDtoday Article • Letter to the Editor • SIGINT-y Social Media Page		

(C) The International Security Issues Build-Out	
FROM:  Global Capabilities Manager, ISI (S2C) Run Date: 05/17/2006	
(C) As the Analysis & Production Mission Build Out Strategy was originally envisioned, International Security Issues (ISI) mission was to remain primarily based in Washington. However, as other product line mission plans began to mature, opportunities for ISI to expand its mission capabilities opened. Planning is underway that will involve ISI participation in build-out activities with NSA/CSS Georgia, NSA/CSS Hawaii, NSA/CSS Texas and the European Security Command. The ISI mission is further extended by its relationships with F6 and Second and Third Party foreign partners that provide valuable analytic insights as well as their technical capabilities.	
(U) NSA Washington Mission	
(U) Regional	
(TS//SI) ISI is responsible for 13 individual nation states in three continents. One significant tie that binds all these countries together is their importance to U.S. economic, trade, and defense concerns. The Western Europe and Strategic Partnerships division primarily focuses on foreign policy and trade activities of Belgium, France, Germany, Italy, and Spain, as well as Brazil, Japan and Mexico. The division reporting also provides some key intelligence on military and intelligence activities in some of these countries. The Aegean and Ukraine division works all aspects of the Turkish target - diplomatic, governmental/leadership, military and intelligence.	
(TS//SI) 	
(U) Transnational	
(TS//SI) 	
(TS//SI) 	
(TS//SI) 	
(TS//SI) 	
(S) Build-Out Support to Counterterrorism and Combating Proliferation	
(S//SI) Today, ISI is actively partnering with the Combating Proliferation (CP, S2G) and Counterterrorism (CT, S2I) product lines to incorporate financial intelligence analysis into their mission build-out plans. The idea is to integrate financial analysis with traditional target efforts as opposed to working the target from two separate perspectives, as is done in NSA Washington. ISI's long-term goal is to introduce financial analysis as part of the Intelligence Analysis curriculum so any target can be enriched with the use of financial intelligence. The first CP FTM-trained analyst arrives at NSA Texas in June. NSA Hawaii's CT effort has several analysts who partner with FTM on select Southeast Asia counterterrorism targets.	
(U//FOUO) NSA Texas	
(TS//SI) 	
(TS//SI) 	
SERIES:	

Comments/Suggestions about this article?

	"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 (DL sid_comms)."
	
	DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007