UNIVERSIDADE DE BRASÍLIA

DOUTORADO EM RELAÇÕES INTERNACIONAIS

PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

DISSUASÃO E GUERRA CIBERNÉTICA: ESTUDOS DE CASO NO PARADIGMA DE DISSUASÃO CUMULATIVA

WILLIAN WASHINGTON WIVES

BRASÍLIA

2021

WILLIAN WASHINGTON WIVES

DISSUASÃO E GUERRA CIBERNÉTICA: ESTUDOS DE CASO NO PARADIGMA DE DISSUASÃO CUMULATIVA

Tese apresentada ao Programa de Pós-Graduação em Relações Internacionais da Universidade de Brasília como requisito para obtenção do título de Doutor em Relações Internacionais.

Área de concentração: Política Internacional e Comparada
Linha de pesquisa: Segurança Internacional e Democracia

Orientador: Professor Dr. Alcides Costa Vaz

BRASÍLIA

2021

WILLIAN WASHINGTON WIVES

DISSUASÃO E GUERRA CIBERNÉTICA: ESTUDOS DE CASO NO PARADIGMA DE DISSUASÃO CUMULATIVA

Tese aprovada pelo Programa de Pós-Graduação em Relações Internacionais da Universidade de Brasília em 10/12/2021 como requisito para obtenção do título de Doutor em Relações Internacionais.

_____

Alcides Costa Vaz
Orientador -IREL/UnB

_____

Marcos Aurelio Guedes de Oliveira
Membro externo – UFPE

_____

Jorge Henrique Cabral Fernandes
Membro externo – CIC/UnB

_____

Juliano da Silva Cortinhas
Membro interno – IREL/UnB

_____

Antônio Jorge Ramalho da Rocha
Suplente – IREL/UnB

BRASÍLIA

2021

*Ao meu avô, Ferdinando Morandi, que sempre soube a importância da educação, descanse em paz, nonno***.**

RESUMO

O domínio cibernético de guerra vem despontando nos últimos anos como a próxima fronteira em ações agressivas entre os Estados. Nesse sentido, destaca-se a importância de dissuasão entre países com vistas a impedir perdas por ações de adversários conduzidas no novo domínio. Demonstra-se que as teorias tradicionais de dissuasão não são suficientes para compreender as possibilidades apresentadas pelos fenômenos; portanto, sugere-se, como alternativa analítica e contributo original da tese, o recurso à teoria de dissuasão cumulativa para análise dos casos mais emblemáticos de conflitos no meio cibernético. Na presente tese são analisados os casos do Solar Sunrise, Moonlight Maze, da Estônia em 2007, o Stuxnet no Irã em 2009/2010, a influência Russa nas eleições estadunidenses em 2016 e o caso da Ucrânia em 2015/16/17. O estudo aponta a pouca efetividade das teorias tradicionais de dissuasão no domínio cibernético para a compreensão do fenômeno e a importância do pensamento de dissuasão cumulativa como alternativa analítica. Ao final, e a partir das contribuições da tese, uma nova conceituação de dissuasão é proposta.

Palavras-chave: diplomacia coerciva - domínio cibernético - armas cibernéticas - dissuasão.

ABSTRACT

Cybernetic warfare has emerged in recent years as the next frontier for aggressive action between states. In this sense, the importance of deterrence between countries is highlighted in order to prevent losses in the new domain by actions of adversaries. It is argued that traditional deterrence theories are not sufficient to comprehend all the possibilities of the new phenomena, so it is suggested to use the cumulative deterrence theory to understand the cases presented. In this thesis, the most emblematic cases of conflicts in the cyber environment will be analyzed, from the Solar Sunrise of 1998 to Ukraine in 2015/16/17, through the cases of Moonlight Maze, Estonia in 2007 and Stuxnet in Iran in 2009/2010 and the Russian influence in the US elections in 2016. It will be demonstrated the little effectiveness of traditional theories of deterrence in the domain, and the importance of cumulative deterrence thinking as an analytical alternative. At last, and building upon the arguments from the thesis, a new concept of deterrence is presented.

Key words: coercive diplomacy - cyber domain - cyber weapons - deterrence.

LISTA DE TABELAS

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

Os Estados modernos são dependentes das tecnologias de informação e comunicação em diversos campos. Inicialmente, essa dependência poderia ser caracterizada em seu aspecto econômico, mas agora está presente também nos âmbitos político e militar. Com isso, há possibilidade de um novo espaço ou domínio, de guerra: o cibernético. Esse estudo busca verificar como a prática da dissuasão entre países (*deterrence*, no termo em inglês[1]) é modificada com a inclusão do domínio cibernético, como isso difere da compreensão tradicional acerca da dissuasão[2] entre atores do sistema de nações e quais as implicações para o conceito de dissuasão podem ser derivadas dessas mudanças. Esta tese pretende analisar e discutir essas diferenças, visando às atividades dos atores e as arenas em que os conflitos se desdobram. Serão estudados os casos mais impactantes de ações ofensivas no meio cibernético envolvendo Estados: Estônia em 2007, *Moonlight Maze*, *Titan Rain*, os ataques cibernéticos à Ucrânia em 2015 a 2017, entre outros. Também será dado destaque ao caso mais destrutivo de conflito cibernético até agora conhecido: o caso da utilização do vírus Stuxnet no Irã em 2009 e 2010.

Conflitos entre Estados na arena cibernética são analisados como possibilidade desde os anos 1980, e os primeiros ocorreram por volta dos anos 2000; porém, ganharam proeminência em 2007 com os ataques cibernéticos em larga escala à Estônia. Desde então, uma série de ações agressivas no espaço cibernético vêm ameaçando a segurança de diversas nações, desde ataques diretos, como o vírus Stuxnet, criado para destruir equipamentos de enriquecimento de urânio no Irã, até vazamentos de informações sigilosas em larga escala, passando por ataques com enormes perdas econômicas, como o vírus *notPetya* na Ucrânia em 2017. Argumenta-se que casos de interferência em processos democráticos se enquadram também nessas categorias (na categoria de ataques do tipo *subversão*).

---

[1] Existem outras possibilidades de tradução do termo, "dissuasão" será a utilizada neste trabalho, embora, em língua inglesa, o conceito de *dissuasion* possa ser diferente do de *deterrence*. Joseph Nye Jr.(2017) utiliza os termos de maneira intercambiável, enquanto King Mallory(2018) os coloca em um mesmo continuum de uso de força coerciva – em um espectro de estratégias - com *dissuasion* possuindo um grau menor de força do que *deterrence*. Em relação à tradução, diversos documentos oficiais da União Europeia publicados em inglês e português traduzem o termo *deterrence* como *dissuasão*. Ver, por exemplo, o documento "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", vertido oficialmente ao português como "COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU E AO CONSELHO Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE". (Disponível em <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52017JC0450> Acesso em 02.jul.2021)

[2] Essa compreensão tradicional será exposta no primeiro capítulo.

Outros ataques cibernéticos ocorreram além desses primeiros exemplos, e estes possuem características em comum que envolvem: a amplitude do ataque, a dificuldade de atribuição a uma entidade específica, como um governo ou grupo, e a dificuldade em se defender rapidamente, mesmo após a sua descoberta. Enquanto isso, alguns países, dentre os quais China e Israel, declararam possuir unidades voltadas a estratégias de combate cibernéticos, com usos possivelmente duplos, de defesa e ataque. Após os ataques de 2007 à Estônia, a OTAN criou um centro de segurança cibernética com base nesse mesmo país[3].

Existem variadas definições de ciberespaço, ciberataques e armas cibernéticas. Neste estudo opta-se pela definição de ciberespaço e ataques cibernéticos de Liaropoulos (2010):

> *"Ciber espaço é o conjunto das redes de comunicação com as bases de dados e fontes de informação no sistema global virtual. (...) Ataques cibernéticos são ataques que são feitos nesse meio com alvos militares ou civis, com objetivo de interromper ou destruir serviços ou capacidades operacionais do alvo"*[4]. (LIAROPOULOS, 2012, p.42)

Essa definição é corrente e variações são encontradas também em autores como Schimmit (2012) e Lin (2012). Esta definição foi escolhida por dois motivos: em primeiro lugar, por ela excluir atividades civis de âmbito meramente criminal de ganho econômico. Em adição, ela é ampla o suficiente para abarcar novas ações que possam surgir no meio, não focando nas ferramentas e técnicas existentes atualmente.

O caso Stuxnet, no Irã, é emblemático para o estudo de dissuasão em caso de guerra cibernética, pois possui elementos de comparação com atividades tradicionais de guerra, ao mesmo tempo em que envolve uma nova maneira de agir até então não adotada por grandes potências (ZETTER, 2015). O caso é interessante, pois pode também ser analisado desde variados pontos de vista, dentre eles, a falha dissuasória do Irã contra ataques cibernéticos, a falha da dissuasão dos EUA e Israel contra ações específicas feitas pelo Irã (enriquecimento de urânio para produção de armas atômicas) e os desdobramentos resultantes dos ataques.

Além do caso do Irã serão estudados outros casos de incidentes cibernéticos, contemplando uma linha do tempo que começa em 1998, com o caso conhecido como *Solar Sunrise*, e que se estende até o ataque à Ucrânia em 2017. Cada um dos casos analisados

---

[3] NATO Cooperative Cyber Defence Centre of Excellence. (https://ccdcoe.org/)

[4] Tradução livre. Ver também: "*Cyberspace refers to the fusion of all communication networks, databases and information sources into a global virtual system and cyber-conflict is defined as cyberspace-based attacks on the civilian and military infrastructures (...) upon which societies and armed forces increasingly depend."* (LIAROPOULOS, 2010., p177) Por extensão, armas cibernéticas são as armas utilizadas para a realização desses ataques.

adicionará elementos à análise, e será útil para prover diferentes pontos de vista sobre o tema. Com base nestes casos, serão estudadas hipóteses subjacentes ao tema derivadas da literatura.

Espera-se, com esta tese, acentuar a importância do domínio cibernético para o campo de estudos de Segurança Internacional e contribuir para o reconhecimento de seu efetivo impacto no cenário da segurança global. Objetiva-se também contribuir para o estudo dos paradigmas de compreensão da dissuasão, ao questionar concepções tradicionais desenvolvidas após a Segunda Guerra Mundial e explorando ideias, que se pretende, mais aplicáveis ao mundo atual, com todas as implicações abarcadas pela existência de um novo domínio de guerra. Espera-se que essa evolução possa ser percebida nos âmbitos conceituais e práticos, tanto como uma maneira de se entender o fenômeno pelos analistas como uma postura a ser adotada pelos responsáveis pelas estratégias de defesa dos Estados, embora entenda-se que a ambição conceitual seja mais factível a um trabalho acadêmico.

O objetivo geral da tese é analisar como a dissuasão (*deterrence*) e a prevenção de ataques e a sua contenção podem ocorrer e como são modificadas pelas novas possibilidades no domínio cibernético, domínio este muito distinto daqueles em que mecanismos dissuasórios ou preventivos tradicionais demonstraram sua eficácia até um passado recente. Objetiva também analisar como as novas tecnologias são assimiladas no cálculo dissuasório dos países e suas consequências para a dissuasão. Para tanto, serão considerados o histórico das ideias de dissuasão e as concepções modernas de dissuasão e novas tecnologias. Recorrer-se-á a estudos de caso, como o do vírus *Stuxnet* no Irã, ocorrido entre 2009/2010, tido como emblemático do potencial destrutivo das armas cibernéticas, em conjunto com a análise de outros casos que ocorreram antes, como o da Geórgia em 2008 e o da Estônia 2007 e depois dele, como os casos da Ucrânia a partir de 2015. Para a análise do Stuxnet será desenvolvida uma metodologia, com definições precisas das variáveis dependentes e independentes e as hipóteses para o caso e que são apresentadas no capítulo três.

Entende-se que os casos de conflitos cibernéticos existentes possam comunicar mais sobre prevenção e contenção, e menos sobre dissuasão, ainda mais em se tratando dos contextos em que se desdobram. Entretanto, para a análise da dissuasão, serão feitas inferências, a partir das evidências e elementos de estudo analisados.

Como ponto de partida, a teoria de dissuasão cumulativa (TOR, 2017) será explicitada no primeiro capítulo para um paradigma alternativo para compreensão do fenômeno. Essa alternativa paradigmática, que abarca possibilidades de trocas constantes de ações agressivas

sem considerá-las necessariamente como falhas de dissuasão em um ambiente de aprendizagem mútua entre os atores, é baseada na ideia de dissuasão cumulativa Israelense. Ela foi apresentada por Tor como uma solução prática e conceitual para o estudo da dissuasão cibernética em contraposição às ideias tradicionais de dissuasão. Nesta tese, as ideias propostas por Tor serão aplicadas aos casos como teste de campo. Para além da demonstração inicial de Tor como alternativa teórica, não foi identificado no restante da literatura a aplicação sistemática desta teoria em uma série de casos, como será desenvolvido nesta tese.

O problema central da tese é: Como a prática da dissuasão entre Estados é alterada pela emergência do domínio cibernético em conjunto com suas novas armas e possibilidades? E ainda: O que decorre da inclusão da dimensão cibernética no repertório da dissuasão tradicional? A conceituação inicial de dissuasão deve ser modificada a partir destas reflexões?

A hipótese inicial é de que a dissuasão tradicional não é eficaz em contextos de guerra cibernética, e que nova forma de dissuasão precisa ser adotada. Considera-se, secundariamente, que as armas cibernéticas são incluídas como opções dissuasórias, da mesma maneira com que diferentes armas com diferentes potenciais destrutivos (ou ainda, diferentes potenciais estratégicos e táticos) seriam incluídas em um cálculo militar convencional, e que, por essa via, o cálculo dissuasório é alterado. Não se argumenta, entretanto, que as ferramentas da dissuasão convencional sejam completamente ineficazes neste contexto, como o fazem alguns autores que serão analisados na seção de revisão de literatura e no primeiro capítulo desta tese. O argumento aqui oferecido é de que o entendimento da dissuasão, e principalmente, das conceituações dos significados do que representa uma falha ou um sucesso dissuasório, devam ser modificados para abarcar as possibilidades advindas do surgimento das armas cibernéticas.

Pelo ponto de vista da discussão de dissuasão entre domínios (*Cross Domain Deterrence* - CDD), a ser definida no próximo capítulo, o domínio cibernético abarca duas possibilidades iniciais para a dissuasão: a primeira é ser tida como ferramenta a ser utilizada nos domínios tradicionais (terra, mar e ar); a segunda, é tê-lo como um domínio adicional, onde a dissuasão deva ser exercida. Essa dualidade é expressa por Schneider (2019), e será presente em diversos momentos nas discussões apresentadas nesta tese:

> *"(...) the delegation of cyberspace as a domain makes cyber operations both a tool to use across conventional domains of warfare and a domain from which operations must be deterred".* (SCHNEIDER, 2019, p.99)

Por fim, cabe notar que as teorias de dissuasão que são frequentemente utilizadas para construção de posturas de defesa de países, foram desenvolvidas, como teorias formais, em um período muito específico da história mundial, durante a Guerra Fria. Essas teorias têm o seu espaço e se demonstraram razoavelmente eficazes ao longo dos anos, entretanto, a emergência do novo domínio requer que o entendimento seja modificado.

Para além de uma postura prática de políticas de Estados, é importante analisar as consequências teóricas e conceituais, ao mesmo tempo em que se delineia uma análise que permita calcular os resultados das posturas dissuasórias adotadas pelos países. Por se tratar de um conceito moldado constantemente pela prática, as análises, por muitas vezes, envolvem a construção teórica a partir da prática e dos exemplos observados. Porém, parte da observação se torna difícil na medida em que, muitas vezes, o fenômeno vai tratar de *ações não tomadas.*

A fim de se atingir esses objetivos, será elaborada inicialmente uma análise teórica do tema, começando com o desenvolvimento das ideias de dissuasão desde o início da Guerra Fria. O capítulo 1 será dedicado a esta análise, incluindo a demonstração da ideia de dissuasão cumulativa dentro de seu contexto teórico. No capítulo 2 serão estudados oito casos de operações cibernéticas com diversos atores, começando com o caso Solar Sunrise em 1998 e indo até a influência russas nas eleições estadunidenses e os casos ocorridos na Ucrânia em 2015, 2016 e 2017. O capítulo 3 será dedicado exclusivamente à análise da utilização do vírus Stuxnet no Irã, incluindo a definição da metodologia para a análise deste caso que se demonstrou como um importante catalizador das análises mais aprofundadas sobre o tema de segurança cibernética. Por fim, o capítulo 4 adicionará elementos além dos casos apresentados para o estudo do tema, mas fundamentais para a compreensão em prazos mais longos dos seus impactos, como novas tecnologias e desdobramentos diplomáticos das relações dos principais atores.

1. DISSUASÃO

Neste capítulo serão analisadas as teorias de dissuasão surgidas após a Segunda Guerra Mundial e como elas se modificaram ao final do século XX e início do século XXI, incluindo a relação mais recente entre dissuasão e armas/operações cibernéticas. Esta análise servirá de base para a compreensão da evolução do fenômeno como um todo, para a análise dos casos no capítulo 2, dos eventos reportados no caso do vírus Stuxnet no Irã (a ser analisado no capítulo 3), e como estes se aproximam ou se distanciam dos modelos propostos para análise de dissuasão ao longo do tempo.

Embora a questão da dissuasão nuclear tenha sido muito estudada na Guerra Fria, dois pontos importantes para a análise do fenômeno aqui proposto – guerra cibernética – não foram estudados a fundo pelos principais autores no período: o desenvolvimento de armas com *menos* poder de destruição que armas atômicas e a dissuasão envolvendo potências sem capacidade de desenvolver armas nucleares. O estudo da dissuasão adaptou-se às novas realidades dos últimos trinta anos e é utilizado em relação às guerras cibernéticas e ao ciberespaço[5]; entretanto, é fundamental compreender a origem do conceito, e quais de seus elementos foram modificados ou permaneceram os mesmos. É importante também verificar quais elementos podem guiar incorretamente a análise ou levar a caminhos analíticos sem saída.

O entendimento de como a Teoria dos Jogos definiu o estudo da dissuasão na segunda metade do século XX e as críticas ao seu desenvolvimento será fundamental para definir, em capítulo posterior, as escolhas metodológicas para as análises dos casos estudados. Entendem-se as limitações subjacentes a qualquer modelagem. Uma simplificação ajuda a entender um fenômeno, porém não irá necessariamente defini-lo ou esgotá-lo, principalmente em se tratando de fenômenos sociais. No caso de fenômenos *complexos*, ao invés de meramente *complicados*[6], qualquer análise que almeje poder explicativo além das restrições do modelo pode ser invalidada por desenvolvimentos posteriores ao estudo e que são, por sua natureza, imprevisíveis. Entretanto, o exercício não é invalidado, pois se espera atingir conhecimentos

[5] "Since the late 1940s, most works on deterrence have been dedicated to nuclear weapons associated with conventional means such as aircraft, ships, and tanks (conventional deterrence having been part of the overall deterrence doctrine all along, particularly in the United States). Today, deterrence faces a broader spectrum of challenges, and space and cyberspace are among them. Both domains have gained a new prominence and deserve serious attention. (…)" (DELPECH, 2012, p.141)

[6] "(…) I define complexity as a condition of nonlinear and/or recursive relationships between causes and effects, which consequently 'limits the ability of individuals to identify the full set of possible outcomes or assign probabilities to particular outcomes of specific actions' (POTEETE et al, 2009, p.103). (…) a complicated system is amenable to scientific reductionism: one can understand the system by disaggregating the whole into its constituent parts, studying them and their interrelationships." (ERNEST, C., 2015, p.32)

acerca do tema, o que ajudará a guiar a análise e os processos decisórios relativos a ele, analisando e ao mesmo tempo moldando-o[7].

Este capítulo pretende analisar a continuidade das ideias sobre dissuasão desenvolvidas na Guerra Fria em contextos recentes, e a sua evolução após os desenvolvimentos das últimas décadas. Serão analisadas duas principais questões acerca do entendimento contemporâneo sobre as armas cibernéticas. A primeira diz respeito à possibilidade ou impossibilidade de dissuasão no campo cibernético. A segunda entende as armas cibernéticas como fator que altera o cálculo dissuasório; em outras palavras, como podem tais armas ser utilizadas para dissuadir. Também será introduzida e analisada uma nova abordagem: a ideia de dissuasão cumulativa proposta por Tor (2015).

A ideia de dissuasão cumulativa é importante para este trabalho, pois esta abordagem propõe o emprego de ações retaliatórias como instrumento comum e não excepcional, não sendo isto considerado um insucesso dissuasório. Além disso, a aplicação das ideias de dissuasão cumulativo abre um espaço de possibilidades de ações dissuasivas para casos de ataques de baixo impacto, além das opções tradicionais de sanções diplomáticas e/ou econômicas, adicionando as armas cibernéticas ao leque retaliatório como opção factível, pelo menos em determinados casos. Argumenta-se que o paradigma de dissuasão cumulativa é fundamental, pois pode prover insumos para a compreensão de longo prazo do fenômeno, além de ser prescritivo em relação a como os Estados devem se portar ao encarar a o emprego de armas cibernéticas e a dissuasão nesse domínio. Ao final, argumenta-se que a dissuasão cumulativa provê uma saída teórica para vários dos desafios identificados no meio cibernético, permitindo uma análise compatível com as ideias correntes sobre Segurança Internacional.

1.1. DEFINIÇÃO E CONCEITOS

Variadas definições de dissuasão são encontradas na literatura, podendo ser mais gerais, abarcando uma diversidade de possibilidades de ações militares ou não, como a de Nacht, Schuter e Uribe:

> "'*Deterrence' is defined as a threat intended to dissuade an adversary from doing something it was planning to do. Such threats are 'if, then' propositions: if you do x then you will be punished with z"*. (NACHT; SCHUSTER; URIBE, 2019, p.30)

[7] Na análise aqui desenvolvida, em alguns pontos, é difícil se desvencilhar de uma certa prescritividade, isto é, uma normatização.

Esta definição carece de uma diferenciação de ações indesejadas fora da esfera militar ou de ações consideradas agressivas (com potencial de danos substanciais a infraestrutura ou estruturas de funcionamento dos Estados ou perda de vidas humanas), abarcando ações econômicas ou até mesmo ações culturais indesejadas[8].

Powell (1990), construindo a partir de Snyder (1961), define dissuasão como uma forma de coerção, restringindo a ações consideradas como ataques e ligando o potencial dissuasório à capacidade de impor custos:

> *"Deterrence is a form of coercion. A state deters an adversary from doing something like attacking by convincing it that the cost of doing so would be greater than the potential gain".* (POWELL, 1990, p. 15)

Morgan (2003) também propõe uma definição mais restrita a ataques militares, e argumenta que algumas definições anteriores são muito amplas ou analiticamente não satisfatórias, com a possibilidade de ataques a qualquer momento, a não ser pelas ameaças:

> *"(...) in a deterrence situation one party is thinking of attacking, the other knows it and is issuing threats of a punitive response, and the first is deciding what to do while keeping these threats in mind."* (MORGAN, 2003, p.2)

Analisando a Teoria dos Jogos no plano de fundo da dissuasão nuclear na chamada "Era Algorítmica", Lindelauf (2021) define dissuasão e a sua importância para a análise dentro destas teorias:

> "*Game theoretically speaking: deterrence equals one player threatening another player with the goal of preventing him to conduct an aggressive action that it has not yet taken (but appears willing to do). In other words, the aim of deterrence is to influence perceptions and the decision calculus of the opponent to prevent him of doing something undesired. Deterrence is therefore based on the psychological principle of a threat of retaliation. For instance, a nation wants to prevent nuclear first strikes or cyber-attacks and a company aims for the non-entry of competitors to their market. A key point in deterrence theory is credibility: are the threats credible or not. This depends on the attacker's beliefs on the capabilities of the defender. Clearly, any decision maker with enough concern for tomorrow is likely to be moved by deterrent threats. Therefore it is not surprising that deterrence is a major theme of game theory, both in economics and political science game theory plays a role in modelling deterrence*". (LINDELAUF, 2021, p. 423)

A definição de Lindelauf pressupõe a ideia de uma ameaça explícita de uma retaliação, entretanto, como será definido para esta tese, existem outras maneiras de dissuadir

[8] Abarcar qualquer ação indesejada como alvo de dissuasão ampliaria em demasia a quantidade de momentos alvo de ações dissuasórias. Ou ainda, nem toda ação indesejada de um país afeta um potencial adversário a ponto de ser alvo de uma estratégia de dissuasão.

sem esse tipo de ameaça, principalmente em se tratando de dissuasão por negação[9]. Essa definição também carece de um detalhamento claro do que significa uma ação agressiva.

Além destas definições, é importante distinguir o ato de *dissuadir* do ato de *compelir* (*compellence*). Segundo Gartzke e Lindsay:

> "*Deterrence is the use of threats to protect the status quo. Its offensive twin, compellence, is the use of threats to change (or restore) the status quo. Both are types of coercion, the use of threats of future harm to achieve a goal, which is distinct from brute force or operations, the inflicting of harm or shifting of benefits on the present. Coercive threats can inflict punishment or exercise denial; thus the prospects of retaliation or impenetrable defenses might deter an attack, and the prospects of unpleasant penalties or military conquest might compel concessions*". (GARTZKE; LINDSAY, 2019, Introdução)

Portanto, compelir um Estado significa obrigá-lo a agir de determinada maneira. Compelir altera o *status quo*. Por outro lado, dissuadir envolve a manutenção de um determinado status quo; em sentido estrito, quaisquer ações que modifiquem o status quo representariam uma falha da dissuasão de um Estado[10]. *Dissuadir* e *compelir* implicam ações coercivas que podem estar presentes no cálculo estratégico dos Estados. Morgan (2003) chama esse entrelaçamento desses fenômenos de *diplomacia coerciva*[11]. Os fenômenos seriam, de acordo com esse conceito, complementares e inseparáveis[12], e são expressos no conceito de dissuasão cumulativa de Tor (2015), a ser analisado posteriormente neste capítulo.

T. V. Paul define ainda o conceito de *dissuasão complexa* diferenciando a dissuasão no pós-Guerra Fria do modelo anterior e apontando as dificuldades das análises em um mundo não mais bipolar:

> "*As the twenty first century dawned, deterrence had become complex because of changes along several dimensions of the international system: an increase in the importance of multiple- state and nonstate actors; the distribution of power (the United States has a large military edge over all other states in the system, but the system cannot quite be called unipolar); power relationships (these are evolving, although great powers are in a state of relative peace); and goals, ideals, and issues (asymmetric challengers want to alter the regional or international status quo). Deterrence operates best when there is clarity on these elements, while ambiguity in*

[9] "Deterrence by denial strategies seek to deter an action by making it infeasible or unlikely to succeed, thus denying a potential aggressor confidence in attaining its objectives." (MAZARR, 2018, p.2) Em contraposição a *dissuasão por punição,* que envolve uma ameaça direta.

[10] Um Estado que queira modificar o status quo estaria em uma posição mais fraca, portanto essa modificação representa uma perda para o Estado mais forte. (JERVIS, 1979)

[11] Sperandei (2006) analisa o conjunto do fenômeno *deterrence-compellence* e argumenta que eles são "dois lados de uma mesma moeda". É importante notar que o conceito de diplomacia coerciva vai além dessa interação, porém, nesta tese, o foco será no lado da *dissuasão*.

[12] Powell (1990) vai além e declara que no seu trabalho não é feita distinção entre os conceitos.

> *them makes deterrent relationships complex, in the realms of both theory and policy. Structural indeterminacy is thus the root cause of complex deterrence. This indeterminacy manifests itself in the areas of signaling threats, attributing responsibility for hostile actions, and asymmetry of interests as diverse actors are driven by different calculations that are difficult to assess.*
>
> *'Complex deterrence' can thus be defined as an ambiguous deterrence relationship, which is caused by fluid structural elements of the international system to the extent that the nature and type of actors, their power relationships, and their motives become unclear, making it difficult to mount and signal credible deterrent threats in accordance with the established precepts of deterrence theory*". (PAUL, 2009, p. 8)

Paul define os tipos ideais de relações de dissuasão, mas ainda com foco nas grandes potências e em armas de grande impacto, como nucleares, biológicas ou químicas. O advento do domínio cibernético não entra nessa definição feita em 2009[13], talvez por ações neste domínio ainda não terem sido tão impactantes até então; porém, a adição deste domínio certamente não reduziu a complexidade dessas relações.

Mais recentemente, ganha força o conceito de dissuasão entre domínios (*Cross-Domain Deterrence* - CDD). Gartzke e Lindsay (2019, Introdução) definem o conceito da seguinte maneira:

> "*We define CDD as the use of threats of one type, or some combination of different types, to dissuade a target from taking actions of another type to attempt to change the status quo. (...) Thus policymakers may use air strikes to retaliate for terrorism, cyber operations to disable an adversary's command and control or to influence its electorate, target economic sanctions to punish a cyber intrusion, or even migration policy to coerce neighboring states*". (GARTZKE; LINDSAY, 2019, p. 3)

Este conceito define de maneira clara dentro de qual moldura de análise é possível entender as ações dissuasivas que os Estados tomam a partir da inclusão dos domínios mais recentes (espacial e espaço cibernético), em adição às ações conjuntas entre domínios que antes eram tratadas como exceção, em vez de possibilidade. Em adição, a prática de CDD, como argumentado por Gartzke e Lindsay, é muito anterior ao seu detalhamento teórico, embora somente agora seja analisada como tal.

Embora o estudo de dissuasão entre domínios seja recente, o estudo da dissuasão em geral não o é. O fenômeno existe como objeto de estudo antes da metade do século XX[14]. Entretanto, com o advento de novas armas e capacidades destrutivas tornou-se um conceito chave. Além disso, a diminuição da quantidade de atores-chave durante a Guerra Fria

[13] Embora abarque as complexidades geradas pelas novas tecnologias em geral, na forma da "Revolução em Assuntos Militares" (RMA).

[14] Snyder (1961) cita que o estudo sistemático da dissuasão começa cerca de doze anos antes da publicação de seu livro.

possibilitou a utilização de modelos de análise da Teoria dos Jogos, permitindo uma modelagem relativamente simples e de fácil exploração, aumentando sua popularidade e abrangência, tanto acadêmica, quanto política, e até mesmo midiática.

Portanto, as principais discussões acerca da dissuasão e o consequente aumento da sua importância analítica e estratégica se deram na segunda metade do século 20, em consequência dos desenvolvimentos de armas de destruição em massa em resposta à eventualidade de uma guerra nuclear. Um argumento corrente e simplista do sucesso da dissuasão como estratégia é a não ocorrência de uma guerra nuclear. Com efeito, após a Segunda Guerra Mundial, nenhuma bomba atômica foi detonada em contexto de um conflito armado. Ocorreram testes nucleares (que podem ser considerados como parte do fenômeno dissuasório). Porém, reduzir o fenômeno da dissuasão na Guerra Fria a este fato é uma simplificação errônea. As táticas, estratégias e políticas adotadas pelos países detentores de armas nucleares impeliram esse resultado em conjunto. Não parece ser possível dizer que apenas elementos dissuasórios foram capazes de impedir ataques, pois isto implicaria considerar os países participantes como aptos e dispostos a atacar a qualquer momento, tendo apenas o medo de represália como justificativa para sua contenção[15].

Durante a Guerra Fria, houve diversos momentos de aproximação e distanciamento entre as potências ocidentais e a União Soviética e seus países satélites. Embora algumas das situações possam ser analisadas (e talvez até *entendidas*) por meio de cálculos dissuasórios, principalmente em momentos críticos, como a crise dos mísseis em Cuba, outros fatores, como questões políticas internas e externas dos países, ou até mesmo elementos culturais se revelaram mais importantes em vários momentos para conter a escalada de tensões ou de conflitos[16].

A escolha acadêmica desta tese de avançar a partir das teorias de dissuasão da era da Guerra Fria não é arbitrária. Da mesma maneira que as teorias de dissuasão foram respostas aos desdobramentos tecnológicos da época, os desdobramentos tecnológicos mais recentes

[15] Morgan vai além e escreve: "If nuclear deterrence worked during the Cold War it was not because we developed a neat theory and implemented it precisely. The Cold War is not a consistently favorable illustration of the utility of deterrence in either theory or practice. This makes it hard to believe that something implemented in such an uneven, at time incompetent, fashion was primarily responsible for the absence of World War III.(…) The next comment must be that, despite all this, it is probably correct to conclude, as many do, that *nuclear deterrence did indeed work, to a point.* (…)" (MORGAN, 2003, p. 34, grifo no original)

[16] Um modelo para compreensão científica dos eventos poderia, a princípio, levar em consideração uma grande quantidade de variáveis. Entretanto, criar uma "grande teoria unificada" que explique a Guerra Fria não parece ser factível e nem é o objetivo desta tese.

são, por muitas vezes, respondidos com as mesmas ferramentas pelos seus analistas. Como explicado por Gartzke e Lindsay:

> "*Deterrence itself has always been a political problem that depends on interests, power, information, and resolve. Yet deterrence theory arose historically in response to the technological problem of nuclear weapons*". (GARTZKE; LINDSAY, 2019, Introdução, p.14)

É importante também diferenciar a dissuasão em caráter geral da dissuasão imediata. A dissuasão em caráter geral se refere a uma ideia vaga de que ataques podem ser retaliados impondo um preço demasiado elevado ao agressor ou de que as defesas implicarão custos igualmente altos para o atacante. A dissuasão imediata se refere a evitar guerras ou ações iminentes, com a certeza razoável de que o potencial agressor está apto a empreender um ataque a qualquer momento. O pensamento dominante de dissuasão imediata, durante a Guerra Fria, se traduziu na premissa de que o adversário estaria disposto a atacar ao perceber qualquer falha na estratégia dissuasória do oponente. (MORGAN, 2003)

Entretanto, no mundo pós-Guerra Fria, um novo balanço de poder se estabeleceu entre as potências. A dissuasão nuclear, embora ainda seja fator a ser considerado, se tornou menos importante do que outras maneiras de lidar com a agressividade entre os Estados (JERVIS, 2005). Mesmo assim, há autores que argumentam que a dissuasão nuclear ainda permanece como fator fundamental para manutenção da paz entre grandes potências (TERTRAIS, 2018; COLBY, 2013; MEARSHEIMER, 1993).

Contudo, as teorias de dissuasão no contexto da Guerra Fria não devem ser aplicadas da mesma forma e sem modificações para a compreensão do mundo no século XXI. Elas representam um legado de tentativas de simplificação, sistematização e compreensão dos fenômenos próprios daquele momento histórico. E também, como objetivo prático, os seus teóricos tentavam fornecer não apenas explicações, mas "soluções" para os problemas enfrentados pelos Estados. Se estas soluções envolvessem a Destruição Mútua Assegurada (MAD – *Mutual Assured Destruction*, no acrônimo em inglês) isso não era um problema (para alguns). Entretanto, na prática, a relutância dos atores chave em tomar medidas que levassem a isso se mostrou mais influente do que qualquer imposição supostamente racional subjacente às teorias. Em outras palavras, o mundo real era mais complexo e as pessoas que tomavam as decisões eram mais hesitantes e mais apreensivas em relação às consequências finais de seus atos, independentemente do que a matemática da teoria lhes indicava.

Em situações de menor agressividade e potencial destrutivo, os cálculos dissuasórios revelaram menor capacidade de explicar as ações dos atores; não por acaso, o estudo de dissuasão ganhou impulso considerável apenas após o advento da bomba atômica. Porém, mesmo em se tratando de situações menos destrutivas, a análise da dissuasão ainda assim pode ser uma ferramenta importante, pois cria modelos manejáveis de fenômenos complexos. Além disso, as ideias subjacentes às teorias de dissuasão de fato orientaram parte importante das estratégias de defesa de vários países, como EUA e Rússia, e os mesmos termos ainda são frequentemente citados, muitas vezes sob novas conceituações e em novos contextos.

Portanto, e a partir da discussão conceitual demonstrada, nesta tese é delineada uma definição inicial mais específica, mas não inteiramente restrita, construída a partir das definições presentes na literatura. Dissuasão é definida como a capacidade de um Estado em evitar ataques ou ações agressivas contra si, por meio de sua capacidade de resposta, defesa ou resiliência, envolvendo a capacidade de impor um custo substancial à outra parte, seja por danos cinéticos, diplomacia ou medidas econômicas, ou o custo imposto por meio da capacidade de resistir a ataques substantivos sem grandes danos (dissuasão por negação). Dissuasão implica a resolução de um jogo, como definido pela Teoria dos Jogos (SCHELLING, 1960), em que os atores principais são os Estados e os resultados se traduzem em paz ou diversas ações agressivas, incluindo conflitos em variados graus. Ações agressivas são aqui definidas como ações com o potencial de gerar danos substanciais à infraestrutura física de um país, danos à estrutura de funcionamento do Estado e da sociedade civil (física ou não), ou perda de vidas humanas.

A vantagem da utilização dessa definição, em se tratando do domínio cibernético, é abarcar, por exemplo, um ataque cibernético voltado à interrupção de serviço de energia elétrica de um país ou um ataque voltado à redução da confiança da população nas estruturas democráticas. Ao mesmo tempo, ela exclui crimes cibernéticos comuns, como subtração de recursos de contas bancárias individuais, pois esses não têm o objetivo de minar as estruturas de funcionamento de um país ou de gerar vantagens estratégicas entre Estados. A discussão acerca desses limiares pode existir, mas será argumentado como os casos demonstrados nessa tese apontam de maneira mais clara para ações do primeiro tipo.

Entender o porquê de as agressões entre Estados continuarem a ocorrer não é um objetivo de pesquisa factível para o presente estudo; geralmente se assume, no campo das Relações Internacionais, que algum tipo de conflito irá ocorrer. Porém, analisar as possibilidades de cálculo dissuasório em determinados contextos pode fornecer chaves de

entendimento importantes para a atuação dos atores, das escolhas que tomaram e, em última instância, do desfecho de determinados conflitos. Atualmente, o campo cibernético e suas armas passam a fazer parte desse cálculo, e suas implicações serão analisadas em seguida.

Ainda há que se diferenciar o conceito em si e a forma como ele é posto em prática pelos Estados. Cada país possui seus documentos de defesa com definições próprias. Entretanto, mesmo esses documentos são indicativos das posturas adotadas em situações práticas. Em certos momentos, a diferença pode ser analisada e as definições podem ser atualizadas ou as implicações dessas posturas podem ser estudadas. Não cabe aqui, entretanto, uma crítica da discrepância entre as práticas e os conceitos; assume-se uma definição básica congruente com a generalidade das posturas de dissuasão presentes entre os países. Os casos serão analisados de acordo com essa definição e a sua pertinência e apropriação poderão ser testadas, tanto em termos conceituais quanto em termos de práticas dos Estados. Ao final da tese a definição de dissuasão será resgatada e sua formulação será adaptada a partir das percepções angariadas ao longo do desenvolvimento e discussões apresentadas.

1.1.1. Dissuasão, Teoria dos jogos e Racionalidade

A dissuasão se baseia na premissa de que os atores irão agir racionalmente em ocasiões específicas. A definição de dissuasão envolve um ator A levando um ator B a crer que um ataque de B a A teria custos muito altos para B em sua análise de custo-benefício do ato. Isso implica que o ator A entende o cálculo que o ator B fará, e acredita que a sua tentativa de modificar esse cálculo será levada em consideração pelo ator B. Mesmo que um ator aja irracionalmente, de modo geral, um dos argumentos para a manutenção das capacidades dissuasórias de um Estado é o de levar esses atores pretensamente irracionais a uma racionalidade, pelo menos no momento de cogitar e, possivelmente, empreender um ataque.

Alguns autores, a serem analisados a seguir, entendem o papel da irracionalidade, e seu uso deliberado em determinados casos. Entretanto, os modelos desenvolvidos pelos teóricos da dissuasão no contexto da Guerra Fria assumem, em geral, essa racionalidade ou, no máximo, o uso instrumental da irracionalidade. Esta simplificação permite modelagens matemáticas importantes.

Em 1960, Snyder procedeu à análise inicial do impacto da irracionalidade. Para ele democracias teriam muita dificuldade em utilizar a irracionalidade de maneira instrumental,

pois seria fácil verificar um possível blefe. Governos autoritários, por outro lado, poderiam utilizar essa tática de maneira mais eficiente por se tratar de decisões, que para serem efetivas, deveriam ser de conhecimento do menor número possível de agentes. Ele argumenta que a racionalidade pode, portanto, ser nivelada de acordo com a situação, mas que democracias tenderiam a ser racionais na maior parte do tempo.

Ao levar ao limite as ideias de racionalidade dentro de determinados modelos, Morgan (2003) conclui que esses modelos são, de fato, inconsistentes ao assumirem a racionalidade dos atores. A dissuasão efetiva dependeria da irracionalidade ou de uma incerteza sobre as ações de, pelo menos, um dos atores; caso contrário, argumenta Morgan, a dissuasão não surtiria resultados. Em um cenário de racionalidade perfeita e informação perfeita os atores saberiam de antemão os resultados de ações e o equilíbrio poderia ser calculado, resultando em diversas situações em que um ataque total e imediato passaria a ser a melhor solução. Obviamente, nenhum ataque desta categoria aconteceu durante a Guerra Fria ou depois.

Jervis (1979), por outro lado, argumenta que a dissuasão funciona mesmo em contextos de baixa racionalidade. Para o autor, a racionalidade pode não ser nem necessária nem suficiente para a teoria, pois a irracionalidade pode ser utilizada tanto para manter uma paz irracional quando para iniciar uma guerra impulsiva. Ele critica diversos aspectos da teoria, entre eles, a questão dos incentivos positivos, e como eles também podem ser utilizados para dissuadir. Como a dissuasão tenta modificar os valores dos resultados de um conflito, incentivos positivos podem alterar este valor, tanto quanto incentivos negativos. Entretanto, segundo Jervis, a maioria dos teóricos, até aquele ponto no desenvolvimento das teorias de dissuasão, ignorava o impacto dos incentivos positivos.

Dez anos depois, Jervis (1989) analisou os impedimentos no desenvolvimento de um modelo de utilidade esperada para dissuasão. Para Jervis, a racionalidade ou a irracionalidade dos atores não pode ser fixada, pois leva a uma série de ambiguidades e paradoxos nas teorias. Ao invés, ele propôs soluções advindas da psicologia para lidar com situações em que a racionalidade não é relevante. Em disciplinas ligadas à economia, um ator que age racionalmente obtém ganhos nos mercados, enquanto atores irracionais são, com o passar do tempo, levados a abandoná-los. Porém, em se tratando de Segurança Internacional, a dissuasão se passa em um mercado de oligopólios, em que as ações de qualquer ator influenciam as ações dos demais, e onde as utilidades são difíceis de calcular e sendo até mesmo irrelevantes para alguns atores. Além disso, adicionar ou retirar um ator do mercado

da segurança global suscitaria consequências para os outros atores do sistema, com novos balanços de poder globais e regionais sendo modificados.

Em síntese, a questão da racionalidade dos atores não foi resolvida e diversos argumentos podem ser razoavelmente convincentes para cada caso. Uma maneira alternativa de se entender determinados fenômenos sociais pode ser a partir da análise de sistemas complexos. Segundo Kavalski (2015), um sistema social complexo é altamente reativo a certas perturbações, ao mesmo tempo em que pode ser altamente resistente a choques e impactos externos. Uma solução para diminuir a necessidade de presunção da racionalidade poderia ser: reduzir a importância das decisões individuais dos atores, em contraste com a análise das interações dos sistemas. Entretanto, em alguns casos, um único ator ou uma quantidade muito reduzida de atores pode tomar decisões-chave que afetam o sistema de maneira óbvia (como a decisão de um presidente de atacar com uma arma atômica). Então, comparar o cálculo dissuasório a um fenômeno similar a sistemas caóticos poderia levar à relativização da importância da presunção da racionalidade. Assumindo que a resposta a uma decisão dessas possa ser feita por um único ator ou um número reduzido de atores, a racionalidade ou a falta dela teria novamente grande importância analítica no modelo. Assumir a necessidade de análise psicológica individual de cada ator impede uma modelagem precisa dos acontecimentos.

Zagare (1990) analisa a diferença de abordagem entre entender a racionalidade como *instrumental* contra entendê-la como *procedimental*. Entender a racionalidade como procedimental implicaria assumir uma capacidade analítica perfeita aos tomadores de decisão, capaz de avaliar a miríade de alternativas possíveis para cada caso, desassociada dos erros humanos comuns de percepção. Zagare argumenta que as críticas à racionalidade nos modelos de dissuasão assumem em geral essa visão procedimental. Segundo o autor, na prática a visão adotada, mesmo que não de maneira explícita pela maioria dos analistas, é a visão instrumental da racionalidade dos atores. Essa visão não seria sujeita a maior parte das críticas, pois parte apenas da ideia de que, dentro de um número limitado de opções, o ator optará por aquela que julga oferecer o melhor resultado. Essa visão só precisaria de dois pressupostos; de que as preferências dos atores sejam conectadas e transitivas, isto é, que ele possa fazer comparações entre elas, e que haja uma ordem entre as preferências (se o ator prefere um resultado A a um resultado B, e prefere um resultado B a um resultado C, logo ele também prefere A a C). Essa visão não diz nada sobre o que um ator *deveria* preferir, tanto

em termos estratégicos como éticos, mas sim sobre como ele organiza e decide sobre uma série de preferências.

Partindo destas argumentações e entendendo a necessidade de se realizar uma decisão analítica, faz-se aqui uma escolha. Para esta tese entende-se um nível de racionalidade suficiente para os atores agirem, na maioria das vezes, de acordo com a expectativa de utilidade marginal, como no conceito econômico. Em situações históricas onde os atores não agiram assim, assume-se a racionalidade limitada e instrumental (*bounded rationality*, no conceito em língua inglesa), ou seja, dentro das restrições de conhecimento que o ator poderia possuir e dentro das percepções de racionalidade instrumental que o ator possuía, o ator em questão toma a decisão que julga ser a melhor, frequentemente a decisão *satisfatória* para aquele momento, em vez da decisão *otimizada*. Existe o risco de que certas decisões possam ser incompreensíveis sem o contexto adequado, que pode incluir aspectos mentais e psicológicos impraticáveis de serem analisados. Entretanto, é um risco que qualquer teoria de análise de decisão deve levar em conta, e, como Lindelauf (2021) argumenta, não se espera que a análise teórica defina sempre como os atores *irão agir*, mas sim como eles *deveriam* agir e que as percepções teóricas sejam mais úteis para a análise dos acontecimentos do que para uma previsão de comportamento de atores específicos.

1.1.2. Schelling, Von Neumman e Morgenstern

Ideias advindas da economia guiaram o estudo de dissuasão na Guerra Fria desde seus primórdios. Em 1953, Von Neumann e Morgenstern publicaram o livro "Theory of Games and Economic Behavior", iniciando o campo de estudos da Teoria dos Jogos. Suas principais contribuições ao campo consistiram na formalização matemática de variados tipos de "jogos" - as regras que regem as interações entre os atores – incluindo jogos cooperativos e não cooperativos, jogos jogados uma só vez ou repetidos e o equilíbrio em jogos de duas pessoas.

As ideias de Neumann e Morgenstern foram fundamentais para o desenvolvimento posterior das teorias de dissuasão na Guerra Fria. Os formalismos matemáticos construídos pelos autores foram escrutinados e replicados por diversos acadêmicos, derivando deles resultados para possíveis cenários e cursos de ação que guiaram políticas, estratégias e táticas militares.

Thomas Schelling continuou na linha do entendimento da dissuasão por meio da Teoria dos Jogos, sendo premiado com o Nobel de 2005 em economia pelas suas

contribuições para o entendimento dos conflitos e cooperação por meio das ferramentas matemáticas desenvolvidas por Neumann e Morgenstern.

Um dos principais pilares da teoria de dissuasão de Schelling (1960) foi a compreensão da guerra como uma situação de *interdependência* e não como de soma-zero. A teoria de Schelling é frequentemente comparada com a teoria dos jogos aplicada aos oligopólios, em que as poucas empresas de um determinado setor competem entre si, não em uma concorrência completamente livre, nem em um estado de monopólio (AYSON, 2004). Neumann e Morgenstern (1953) já haviam trabalhado a teoria dos jogos nos contextos de oligopólios. Entretanto, a inovação de Schelling se traduz em não pensar o jogo de dissuasão como um jogo de apenas dois atores, mas sim de alguns atores que interagem fortemente entre si e fracamente com os atores fora do jogo.

Um mercado monopolístico é caracterizado por não permitir concorrência. Por outro lado, em um mercado de livre concorrência a decisão de uma empresa não afeta as outras. As relações internacionais se assemelham a um mercado oligopolístico, onde as decisões de um agente afetam os outros, mas não há um monopólio da tomada de decisão por um único agente. As relações entre os Estados são intermediárias, não havendo um centro de poder total. Porém, cada ator não é livre para tomar decisões sem pensar nas respostas dos outros atores. Por isso, para entender a dissuasão é importante não se ater apenas à resolução de conflitos entre dois atores poderosos, mas sim entre os diversos atores que possuem alguma capacidade de barganha.

Para Schelling, a guerra é essa situação de barganha, onde conflito e interdependência devem ser considerados em conjunto para a compreensão do fenômeno. As posições de um ator influenciam as dos demais e são influenciadas por elas. Além disso, as próprias expectativas de como cada ator irá agir em resposta a outro influenciam as ações, e assim por diante. Segundo Schelling:

> "*Deterrence (...) is concerned with influencing the choices that another party will make, and doing it by influencing his expectations of how we will behave. It involves confronting him with evidence for believing that our behavior will be determined by his behavior*". (SCHELLING, 1980, p. 13)

Dentro de um processo de barganha, além do cálculo racional é possível considerar os aspectos psicológicos dos atores envolvidos. Considerar as ações de um determinado ator como "irracionais" ou "frutos de uma loucura" ignora o fato de que esse ato pode derivar de um cálculo racional para o ator que o fez. Além disso, entender esses atos como não racionais

seria uma limitação do agente que faz a análise. Em outras palavras, Schelling diz que aparentar ter um comportamento irracional pode ser um método de manipulação. Schelling entende esses fatores, e analisa como eles se posicionam ao desenvolver sua teoria. Entretanto, não avança na análise de situações em que um dos atores ou ambos são irracionais de fato[17].

Schelling analisa como situações de estabilidade e instabilidade surgem dentro do sistema. Uma barganha é entendida como o ponto dentro de uma variação possível em que os atores acreditam e concordam que estão melhores com a aceitação do acordo do que sem ele. Em se tratando de dissuasão entre potências nucleares, é necessário que os atores creiam na existência de um ponto de equilíbrio possível. A possibilidade de destruição mútua total entra, em alguns casos, como fator de estabilização do sistema. Um dos lados tenderia a não deixar o outro crer que as únicas opções para ele são a derrota ou a destruição mútua, pois isso levaria o lado pressionado a escolher a opção de destruição mútua, o que seria ruim para ambos.

Segundo Field (2014), entender e aplicar a posição de von Neumann, um dos principais autores que influenciaram o trabalho de Schelling, implica levar a teoria dos jogos ao extremo e prever a destruição mútua massiva por meio de armas nucleares. Von Neumman entende a guerra nuclear como um dilema do prisioneiro jogado uma só vez, o que implica a solução de Nash, que é não cooperar. Não apenas não cooperar; no caso da dissuasão nuclear, a argumentação que Neumann apresenta é clara: atacar primeiro e o mais rápido possível[18]. Entretanto, aqui se encontram os limites da teoria de Neumann e Morgenstern. Quando apresentada em conjunto com a formalização matemática e o cálculo do equilíbrio do jogo, a posição parece justificada e racional. Porém, diversas barreiras existem para colocar essas ações em prática. Incluem-se nessas barreiras fatores culturais, mentais e psicológicos dos tomadores de decisão.

Neste sentido, Schelling critica a postura de derivar soluções para o mundo real a partir de axiomas. A sua tentativa de estabelecer os parâmetros de comportamento que podem

[17] Isso ainda não gera uma discussão significativa, pois dentro dessa teorização não há uma definição do que significa ser "irracional de fato" e que diferença isso há do comportamento irracional proposital. Ambas as possibilidades levam a decisões aleatórias do agente, gerando imprevisibilidade e consequente impossibilidade de uma modelagem precisa.

[18] Neste contexto cabe citar a frase de Neumann para a revista Life em Fevereiro de 1957, se referindo a um possível ataque nuclear à União Soviética: "*If you say why not bomb them tomorrow, I say why not today? If you say today at 5 o'clock, I say why not one o'clock?*" É interessante notar que, embora Neumann tenha trabalhado até sua morte em 1957 como consultor de segurança dos EUA, este seu posicionamento nunca foi colocado em prática.

guiar o entendimento dos limites da teoria dos jogos levaram a uma primeira aplicação experimental, mas ainda acadêmica. A dissuasão foi um tema inicial que Schelling julgou importante para a aplicação de suas ideias. Entretanto, não é o único tema ao qual elas seriam aplicáveis. E ele mesmo discorreu que a formalização e modelagem, embora instrumentos importantes e interessantes, não seriam capazes de captar todas as dimensões de decisão em um conflito.

A forma de análise introduzida pela Teoria dos Jogos é importante para entender não apenas o fenômeno, mas a maneira como os tomadores de decisão o compreende. A teoria teve uma divulgação tão ampla que influenciou o pensamento e o modo de lidar com as situações de várias gerações de atores importantes dos Estados[19]. Para esta tese, diversas acepções desta teoria serão utilizadas, pois elas guiaram o estudo das teorias e conceitos base aqui presentes. Com a evolução das ideias de dissuasão, a aplicação foi se tornando cada vez mais especializada e os conceitos foram se sofisticando ao longo das décadas. As próximas seções demonstrarão tais desenvolvimentos e especializações.

1.1.3. Dissuasão e Poder

Glenn Snyder (1960,1961) considera a dissuasão como um tipo de poder político. Segundo o autor, o poder seria a capacidade de induzir outros a fazerem ou a não fazerem o que eles fariam ou não fariam. A dissuasão seria um aspecto negativo desta utilização do poder, pela ameaça de aplicar alguma sanção. Portanto, a utilização de dissuasão, como estratégia, levaria a um possível aumento de tensões e diminuição da cooperação entre os Estados.

Snyder analisa a dissuasão em termos mais gerais, levando em conta não só as questões militares, mas também as econômicas e políticas. Ele utiliza o conceito de poder de Robert Dahl para analisar a dissuasão, porém adicionando dois componentes aos quatro iniciais de Dahl (base, meios, quantidade e escopo): valores (*object value*, no original) e credibilidade.

[19] Aqui cabe uma nota acerca da ética subjacente ao fenômeno da popularização da Teoria dos Jogos. As consequências que a utilização e a divulgação de uma teoria que adquiriu tamanha influência nos tomadores de decisão poderiam ser catastróficas globalmente. Uma argumentação muito bem elaborada para um ataque nuclear feita por um pesquisador preocupado com a ética da utilização de seus achados deve ser publicada? As consequências da utilização da Teoria dos Jogos em determinados casos poderiam ter sido muito severas, e em alguns momentos a decisão de atacar ficou apenas nas mãos de poucos atores-chave. Uma teoria alternativa mais convincente teria responsabilidades éticas maiores?

A dissuasão nuclear, em seu nível mais extremo, não se preocupa com os valores dos objetos alvos de dissuasão, apenas com que esses valores sejam grandes o suficiente, como, por exemplo, o valor perdido com a destruição de uma cidade. A credibilidade, por outro lado, é tema recorrente. A credibilidade da ameaça é fundamental para que um oponente racional possa ser dissuadido. A intenção de utilizar determinada capacidade ou força é tão importante quanto sua existência. Snyder argumenta que os EUA não foram capazes de se beneficiar muito das armas nucleares quando eram os únicos detentores da tecnologia, pois os potenciais inimigos não acreditavam na real intenção de seu emprego.

Embora seja um entendimento comum na disciplina de Relações Internacionais de que a guerra é a extensão da política por outros meios (Clausewitz), em se tratando de dissuasão nuclear, qualquer guerra entre as potências nucleares seria uma falha da capacidade dissuasiva não só de um Estado específico, mas de todos os envolvidos. O início de uma troca nuclear entre as grandes potências sinalizaria o fim da possibilidade de guerra e política futura (como Schelling escreve: "*o cancelamento do futuro*"). Isto implica que a guerra nuclear não seria a continuação da política, mas sim o fim total e permanente dela. Snyder argumenta que, mesmo em uma situação de guerra, a dissuasão continuaria a existir, pois um ataque retaliatório atual é uma ameaça de um ataque futuro, com aumento das potenciais perdas do agressor inicial. O modelo de *brinkmanship* de Powell (1990), a ser explicado a seguir, compreende essa continuação da dissuasão ao entender os variados níveis de agressão que culminam com uma guerra nuclear total.

1.1.4. Powell e Credibilidade

O modelo de *brinkmanship* de Powell (1990) é um dos ápices da análise da dissuasão nuclear. Em seu estudo, ele modela diversas situações e fornece soluções matemáticas para os casos explorados. A questão da credibilidade aparece já no título (*"Nuclear Deterrence theory – The Search for credibility"*) e a pergunta acerca de como garantir a credibilidade guia a análise. A análise deste modelo é importante para entender de onde parte uma fração importante do pensamento contemporâneo de dissuasão. Contudo, como será demonstrado no restante da tese, as situações analisadas em termos de dissuasão cibernética estão distantes da destruição termonuclear e precisam ser analisadas pelas suas características de conflitos com potencial destrutivo intermediário e não total. Ainda assim, a análise dos modelos de Powell é útil, pois, ao se tratar da discussão aqui proposta, é de se esperar certa comparação com os

modelos de dissuasão vigentes durante a Guerra Fria. Além disso, o modelo permite uma transição entre as ideias exploradas durante a Guerra Fria e ideias mais recentes de dissuasão.

A principal questão explorada por Powell é a possibilidade de degraus de escalada do conflito. Opções intermediárias fornecem possibilidades para testes da credibilidade dos atores a cada passo, de até onde cada um está disposto a ir antes do limiar de uma guerra nuclear. As opções intermediárias são limitadas, mas sua existência modifica o cálculo. Nos modelos iniciais de Snyder (1960), a matriz de possibilidades para a análise de dissuasão possui apenas quatro resultados, enquanto para Powell os resultados são mais bem diagramados com árvores de escolhas, que podem se estender por muitos ramos para abarcar os diversos resultados possíveis, de acordo com as escolhas disponíveis aos atores.

Powell modela jogos na ausência de informação completa, de estabilidade em contextos de crise e de retaliação limitada, avançando a modelagem dos conflitos. Essa análise possui elementos que podem ser levados em conta ao se analisar dissuasão em situações contemporâneas, mesmo em se tratando de conflitos com menor potencial destrutivo. A ideia de que exista um momento em que o conflito pode decair a um ponto sem retorno pode ser aplicada a situações com grandes interesses, mas sem destruição mútua envolvida.

Uma contribuição importante de seu trabalho é entender que a mera existência de armas nucleares, de capacidades de *second-strike* e de doutrinas de destruição mútua assegurada (MAD) não necessariamente simplificam o cálculo dissuasório, pelo contrário. A possível existência de novas opções dissuasórias também é analisada, com possíveis impactos sendo também objeto de estudo. Entretanto, o foco de análise permanece nas armas nucleares[20].

No modelo de Powell, em um conflito entre potencias nucleares, ambos os atores caminham em direção a um "abismo", e cada passo na escalada do conflito leva ambos para mais perto do ponto de não retorno. Em certo momento, as ações dos atores podem levar a uma descida drástica a esse ponto e, mesmo que algum deles deseje retroagir, a guerra nuclear acontece. O argumento de Powell afirma que os Estados seriam reticentes ao lidar com isso, escalando aos poucos e recuando na menor possibilidade de deslizar ao abismo. Uma das principais vantagens estaria em manter a margem de manobra, com um leque de opções de

[20] Esta é uma postura comum nos autores do período; os conflitos com menor potencial destrutivo não seriam merecedores de análise diante do potencial catastrófico das armas nucleares. Isto pode ser um problema ao se transportar as teorias de dissuasão para contextos contemporâneos, já que o que agora o impacto do que se assume como o risco de fato é bem distante do impacto de uma guerra nuclear.

ações. Uma escalada a um ponto sem retorno do conflito reduz a quantidade de ações a, potencialmente, uma (retaliação e consequente destruição mútua). Neste modelo o caminhar na escada não representa necessariamente uma falha da dissuasão a cada degrau, pois o objetivo principal seria evitar a destruição total e não necessariamente evitar cada etapa intermediária.

Certos casos de conflito podem apontar no sentido de um caminhar cauteloso dos atores. Por exemplo, a relação conturbada entre Índia e Paquistão não produziu uma guerra nuclear, ainda que ambos dominem a tecnologia nuclear. É possível argumentar que um ataque nuclear tenha sido refreado em ambos os lados pelo medo da retaliação do opositor, embora isso não tenha sido o suficiente para diminuir as tensões na região.

A credibilidade entra em cada modelo como fator chave. Um Estado quer se mostrar capaz de levar adiante seus compromissos. Uma das maneiras seria cumprindo compromissos menores, para dar um sinal claro de que compromissos maiores seriam também cumpridos. Entretanto, nada garante que os compromissos sejam interdependentes. Em alguns casos, contra-atacar pode ser contra produtivo uma vez que um ataque inicial tenha sido sofrido. Entretanto, a garantia de um contra-ataque, mesmo quando irracional, é importante para a credibilidade da dissuasão. É interessante contrapor esse fato aos pressupostos de racionalidade dos atores no modelo. Mesmo quando a postura de maior impacto dissuasório é irracional, a racionalidade do outro ator é presumida, resultando em uma contradição se a análise for feita simultaneamente pelo ponto de vista dos dois atores. Zagare (1990) resolve este paradoxo adicionando a ideia de expectativas de incerteza sobre a capacidade do oponente de mudar sua postura previamente compromissada. Neste caso, uma probabilidade de mudança de postura do agredido é adicionada ao cálculo do agressor. Assim, mesmo se tratando de uma escolha racional em não retaliar massivamente, a probabilidade dessa retaliação gera incerteza suficiente para funcionar como dissuasão[21].

Outros analistas argumentam que não há uma solução matemática estável para o cálculo de credibilidade para a maioria dos jogos repetidos (BRAMS; HESSEL, 1984)[22]. E ainda, conforme aumenta a complexidade dos requisitos necessários para uma resposta

[21] "Suffice it to say that the model reveals that when the credibility of each player's threat is 'sufficiently' high, deterrence is likely, though not necessarily certain, as some theorists have speculated." (ZAGARE, 1990, p. 259) Ou seja, a proposta de Zagare permite uma existência de probabilidade de sucesso ou insucesso da dissuasão, levando em consideração a racionalidade instrumental e não procedimental (que levaria a um resultado fechado e certo dentro de uma análise de escolha racional).

[22] Levando em consideração uma racionalidade procedimental dos atores, como argumentado por Zagare (1990).

dissuasória, a credibilidade do emprego de uma potencial resposta diminui consideravelmente (CIOFFI-REVILLA, 1983).

Em adição, os resultados dos modelos apresentam uma modificação ao se considerar novas variáveis, como a repetição dos jogos, as barreiras internas para respostas dissuasórias, o uso instrumental da irracionalidade e a adição de respostas intermediárias. Isso implica as seguintes perguntas: quanta simplificação é possível antes do modelo deixar de ter algum uso no mundo real? E quanta simplificação é necessária para o modelo ser tratável, ou seja, ser matematicamente e academicamente passível de análise e compreensão?

O balanço entre as respostas a essas duas perguntas levará ao menor modelo possível de ser tratado e que ainda seja útil à compreensão da realidade. Não há consenso sobre como este modelo poderia ser desenvolvido. Entretanto, assume-se, em larga medida, que a modelagem em si seja útil. E ainda, ela também expõe as falhas subjacentes ao raciocínio humano, tanto dos cientistas que analisam os fenômenos, quanto dos tomadores de decisão que utilizam ou ignoram essas análises.

1.2. A TRANSIÇÃO PARA AS IDEIAS MAIS RECENTES DE DISSUASÃO E O SEU PAPEL ATUAL

As ideias de dissuasão estiveram, até os anos 90, ligadas à sua expressão *nuclear*. Lowther (2013) argumenta que esta é uma das causas da estagnação dos estudos de dissuasão no pós-guerra fria. Porém, mais recentemente, a definição do Departamento de Defesa dos EUA entende a dissuasão como tendo um escopo amplo[23]. Neste sentido, as acepções atuais de dissuasão ainda misturam a amplitude do conceito com sua aplicação durante a Guerra Fria. Ainda assim, as definições utilizadas comportam indícios de que a conceituação do termo permite ampliar sua apreensão moderna, construindo entendimentos a partir dos elementos criados anteriormente nas décadas da Guerra Fria.

Não obstante a discussão acerca das diversas acepções do termo e da sua conceptualização, os Estados continuam a perseguir alguma capacidade de dissuasão como

[23] "Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, defines deterrence as 'the prevention from action by fear of the consequences (. . .) a state of mind brought about by the existence of a credible threat of unacceptable counteraction.' From this definition it is easy to see that deterrence can incorporate a wide range of means focused on an equally wide array of actors. Unfortunately for deterrence theory, the concept has often been seen as synonymous with Cold War nuclear strategy, which played a major role in post–Cold War stagnation. Efforts are now under way to expand the context in which deterrence may prove useful in defending national interests against a host of new and developing threats." (LOWTHER, 2013, p.3)

objetivo estratégico. O conjunto dos atores envolvidos pode agora ir além dos atores estatais, envolvendo outros como organizações terroristas e grupos paramilitares. Lowther (2013) argumenta que, a princípio, alguns atores podem parecer não passíveis de dissuadir, e que, em alguns casos, a dissuasão deve ser empregada em conjunto com as possibilidades de contenção ou, até mesmo, de erradicação. Entretanto, argumenta também que, na prática, a maioria dos atores são passíveis de serem dissuadidos. A diferença de valores culturais não torna um ator irracional, mas demanda que os termos da dissuasão sejam claros para aquele ator, dentro de um contexto cultural específico.

Embora existam reflexões modernas sobre dissuasão relevantes, as consequências destas discussões não parecem ressoar com a mesma intensidade anterior nas comunicações de Defesa oficiais dos Estados. Documentos de defesa dos EUA[24] e da União Europeia[25] citam a dissuasão como seus objetivos. Entretanto, a dissuasão tal como neles definida, é de caráter geral, e não uma ação iminente que possa ser tomada em resposta a uma agressão. São tratadas, em termos que definem, de maneira ampla, possíveis respostas a possíveis ações que um eventual inimigo possa tomar. Ainda assim, segundo as teorias tradicionais de dissuasão, uma estratégia dissuasória necessita ter credibilidade para surtir efeito, a qual pode ser garantida de diversas maneiras, inclusive com a definição clara de ações que serão tomadas em determinados cenários.

Outra maneira em que a dissuasão pode ocorrer é pela incerteza (MORGAN, 2003; SCHELLING, 1980), em particular, incerteza sobre a extensão de uma possível ação retaliatória. Entretanto, levando em conta a necessidade de adequação cultural para dissuasão de atores imersos em culturas muito diferentes, a incerteza pode levar a falhas da dissuasão. O cálculo racional para um Estado ocidental pode ser formal e baseado em elementos lógicos[26], mas a aparente irracionalidade de determinados atores deve ser compreendida e não abstraída

[24] No sumário da estratégia de Defesa dos EUA a primeira linha já deixa isso bem claro: "The Department of Defense's enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our nation. Should deterrence fail, the Joint Force is prepared to win." (UNITED STATES OF AMERICA. **Summary of the 2018 National Defense Strategy of the Unites States of America**. 2018. Disponível em https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf acesso em 13.maio.2021)

[25] EUROPEAN COMISSION. **JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.** 2017. Disponível em <https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf> Acesso em 13.maio.2021.

[26] Ou não, pois há de se levar em conta que nem todas as decisões são feitas por um agregado de preferências, algumas são frutos de atuações individuais que dependem de flutuações imprevisíveis de personalidades. E mesmo em se tratando de decisões feitas por grupos, situações como a da tragédia dos comuns mostram que o resultado de ações individuais pode ser catastrófico. Entretanto, para essa comparação a simplificação parece ser possível.

como apenas uma impossibilidade epistemológica. Atores aparentemente irracionais podem ser dissuadidos, mas a incerteza pode apenas mascarar uma mensagem que para um ator com o mesmo tipo de racionalidade[27] seria clara.

A dissuasão iminente, no sentido de explicitar claramente o que cada ação de um inimigo irá gerar como resposta, da forma que era mais comum na Guerra Fria, não aparece mais como foco nas comunicações modernas (com objetivos dissuasórios), nem como uma das principais estratégias. A credibilidade da dissuasão em contextos de novas ações, como a guerra cibernética, ainda é questionada, já que as barreiras entre ações agressivas de combate e ações agressivas de propaganda se misturam e que ações de dissuasão críveis por parte dos afetados não foram tomadas ou não surtiram efeitos impactantes (como será analisado nos próximos capítulos). A inação pode representar a complexidade do problema, o medo da escalada de conflitos ou ainda a incapacidade de se dissuadir nestes termos.

Ainda há autores que argumentam que a dissuasão nuclear permanece como um fator importante. Tertrais (2018) argumenta que a dissuasão nuclear ainda é relevante pois as armas nucleares seriam opção com alto custo-benefício para a prevenção de guerras, mesmo levando em consideração desenvolvimentos recentes de novos armamentos. Tertrais repete o mesmo argumento de que em 70 anos não houve um único ataque nuclear e que os países com capacidades nucleares não foram significativamente atacados desde então. Para ele, as alternativas à dissuasão nuclear são invalidadas por sua falta de sucesso nos anos anteriores à existência de armas nucleares. A quantidade e a natureza das guerras, até então, seriam argumento suficiente para declarar a falta de opções à dissuasão nuclear.[28]

Na mesma linha de argumentação de Tertrais encontra-se Colby (2013). Porém, em adição, ele tenta contra argumentar em relação aos fatores que potencialmente reduziriam a necessidade da dissuasão nuclear atualmente. Primeiramente, o autor sustenta que os potenciais ganhos de uma guerra no presente, embora não iguais às guerras passadas, ainda são relevantes o suficiente para mantê-las como possibilidade real para os Estados. Para o autor, o argumento liberal de que o ganho com o comércio livre entre nações é potencialmente maior que o ganho com a guerra nem sempre se sustenta. Para esta argumentação, as ideias de

[27] "Tipos de racionalidade" pode ser entendido de diversas maneiras, mas, um exemplo do que aqui se trata pode ser dado como a diferença de uma cultura que dá um peso maior a religião, neste caso a imagem de uma pretensa "guerra santa" pode ser utilizada com mais impacto do que contra uma cultura mais laica. Entre duas culturas religiosas essa imagem seria entendida e poderia servir de justificativa plausível para uma guerra, enquanto uma cultura laica teria dificuldade em entender a racionalidade subjacente e acharia o que ator é irracional.

[28] Outros autores vão para o lado inverso, e argumentam que a dissuasão nuclear é contra produtiva. (WILSON, 2008)

capitalismo são levadas ao extremo. Um mundo totalmente liberal, segundo o autor, é contrário à natureza humana de querer se unir em grupos, mesmo quando racionalmente essa união faça sentido. Portanto, enquanto existir a potencialidade da dinâmica de "nós contra eles" nas relações humanas, a guerra estaria sempre disponível como forma de conquista de riquezas ou de ganho e consolidação de poder através da força.

O próximo argumento de Colby alega que nem sempre as guerras são feitas por motivos econômicos. Em alguns casos, o medo da posição de adversários pode gerar guerras, mesmo quando o ganho potencial pelo comércio é maior. O exemplo oferecido é o da França no período Entre Guerras, quando a política de isolar a Alemanha - contraproducente em termos econômicos - foi escolhida por outros motivos, adicionada a dinâmicas de punição e revanchismo. Além disso, as ambições de conquistadores individuais também são fatores que levam a guerras que não poderiam ser explicadas em termos econômicos[29].

Colby contrasta o argumento de Jervis de que as comunidades de segurança garantiriam a paz sem a necessidade de armas nucleares, pois embora elas tenham sido essenciais para a construção dessas comunidades, elas agora estão em um caminho de dependência de trajetória (*path dependency*, no conceito em língua inglesa). Nessa dependência, modificar as relações e seguir outro caminho se torna custoso demais, em diversos termos. Colby, entretanto, argumenta que não há garantia de que essa condição irá se sustentar, retomando o argumento de que a natureza humana é, em última instância, causa das guerras[30].

Para Colby, é inevitável e próprio da natureza humana produzir guerras. E ainda, o dilema da segurança – erigir defesas formidáveis leva, ao mesmo tempo, a possibilidades de ataque formidáveis - leva à insegurança constante entre rivais a qual, atualmente, só poderia ser contida com a possibilidade de destruição massiva garantida pelas armas nucleares. O autor argumenta que a paz garantida pelas armas nucleares gera apenas uma falsa *impressão* de que essa paz existe a despeito das armas atômicas.

Para a presente tese, a importância da dissuasão nuclear serve apenas como plano de fundo para as ações dos Estados. Em geral, será assumido que os usos de armas cibernéticas específicas por atores estatais gerem impactos que não sejam suficientes para uma escalada de

[29] Potencialmente poderiam ser explicados em termos psicológicos, mas nesse caso a análise em geral será posterior aos eventos.

[30] O argumento de Colby leva a uma inevitabilidade da guerra por conta da natureza humana, com um pessimismo inerente à essa natureza. A análise aqui desenvolvida não necessita deste aspecto para a explicação do fenômeno. Além disso, há de se apontar que levar este argumento ao seu extremo lógico já foi muito utilizado em diversos pontos da história como justificativa para diversas barbáries.

conflito que chegue perto de uma guerra nuclear. Ainda assim, a dissuasão existe em uma escala contínua, sendo a destruição mútua assegurada um dos seus extremos. Nos degraus que levam ao abismo, como no modelo de Powell, os ataques cibernéticos com fins dissuasórios estão distantes da queda livre. Eles representam passos que tornam mais próximo esse abismo e não é possível excluir totalmente a ideia de que essa possibilidade pode ter sido um fator que evitou um emprego mais pelos Estados.

Caso o motivo do refreamento da utilização indiscriminada de armas cibernéticas pelos Estados seja, de fato, o medo da escalada de conflitos, os degraus que levam ao abismo nuclear poderiam estar mais perto do que o assumido[31]. Neste caso, os atores estariam dando uma importância significativa para a chance de escalada imediatamente subsequente ou, ainda, qualquer troca inicial de agressões teria uma chance razoavelmente grande de ser seguida por agressões subsequentes, até o ponto de não retorno.

Outro ponto a ser analisado é que mesmo conflitos menores tem o potencial de acarretar altos custos aos Estados participantes. Isso pode indicar que os potenciais ganhos com armas cibernéticas seriam menores do que os benefícios da ausência de ataques.

A análise do custo-benefício dos conflitos poderia desmentir a impressão de que as armas atômicas sejam a causa da longa paz entre as potências. Neste sentido, talvez o argumento liberal seja coerente, afinal, caso esse fator de dissuasão sirva para conflitos menores, como os cibernéticos, a diferença para os conflitos maiores não seria qualitativa, e sim apenas quantitativa. Danos maiores envolvem custos maiores com benefícios mais incertos, e ainda haveria dúvidas se de fato existiria ganho algum pelo agressor.

Uma última observação antes de seguir à próxima seção. A contextualização e a factualidade do objeto aqui analisado, durante a Guerra Fria, propiciaram estudos muito profícuos naquele período. Porém, desde então, o universo de atores e estudos sobre o tema ainda não possuem a mesma amplitude atingida ou o mesmo prestígio anteriormente estabelecido. É possível considerar que o debate sobre o tema experimenta uma volta às origens, com a discussão sobre a possibilidade de dissuasão, do papel da racionalidade, e da própria necessidade de se adicionar fenômenos contemporâneos aos cálculos dissuasórios dos países. Isto pode ter se dado devido à diminuição considerável de estudos sobre dissuasão na primeira década no pós-Guerra Fria. A lacuna de aproximadamente dez anos foi interrompida pela volta do interesse analítico pelo tema, nas últimas duas décadas.

[31] Ou os Estados apenas assumem que o abismo estaria mais perto. De qualquer modo, o resultado é o mesmo.

1.2.1. Dissuasão e novas tecnologias

Morgan (2003), ao analisar o que na época era chamado de RMA (*Revolution in Military Affairs*), entende a guerra cibernética como uma das possibilidades em desenvolvimento com grande capacidade de influenciar as guerras contemporâneas e a dissuasão. Em 2003, Morgan elaborou uma análise na qual os elementos de guerra cibernética são entendidos ao lado de outros desenvolvimentos tecnológicos, como a vigilância, o monitoramento por satélite, o desenvolvimento de defesas antimísseis, munições guiadas, *drones* e veículos não tripulados, dentre outros. Para o autor, esse entendimento adiciona elementos intermediários às opções dissuasórias e, consequentemente, aumenta a credibilidade da dissuasão. Outro fator que aumentaria tal credibilidade é a aceitação política maior, nas democracias, de armas mais precisas que causam menos danos colaterais e menos mortes, principalmente mortes evitáveis.

Morgan especula também que, se a revolução nos assuntos militares (RMA) chegasse à maioria dos Estados, uma situação de dominação da defesa poderia ser atingida, ou seja, uma situação em que se defender é muito mais efetivo do que atacar, adicionando assim um elemento de estabilidade ao cálculo dissuasório global. Com armas nucleares, a única opção dissuasória seria a retaliação massiva, pois, somente neste caso a defesa total seria praticamente impossível. Afinal bastaria que algumas armas nucleares passassem pelas defesas do oponente para causar grandes danos. Com a dominação da defesa, o cálculo dissuasório levaria os países a evitar quaisquer ataques, pois estes teriam muito pouca efetividade, sendo desincentivados ao se estabelecer uma análise de custo-benefício.

Por outro lado, o rápido desenvolvimento tecnológico pelas grandes potências militares pode desequilibrar de tal maneira as capacidades militares que Estados menores não enxergariam outra opção a não ser o desenvolvimento de armas nucleares. Morgan cita o exemplo do Iraque e da Índia, sendo este país explícito em dizer que o seu desenvolvimento de armas nucleares é uma resposta à incapacidade de estar à altura das grandes potências militares em outras arenas de desenvolvimento militar. Os desenvolvimentos nucleares da Coréia do Norte poderiam se enquadrar nessa categoria.

Em 2003, quando o livro de Morgan foi publicado, os casos de ataques cibernéticos ainda eram incipientes, ou carentes de informações disponíveis. Hoje se sabe que o desenvolvimento de armas cibernéticas já estava em plena voga naquele ano. Entretanto, para

o cálculo dissuasório dos países até então, a informação na época se demonstrou suficiente para as primeiras análises.

Fortmann e Von Hlatky identificam algumas das vantagens da RMA, sendo a mais interessante para a análise nesta tese a questão da credibilidade de opções de ações intermediárias:

> *"(...) the RMA alters the deterrence equation by reducing the costs associated with intervention should the threat fail to produce compliant behavior. (...) A reputation for resolve enhances credibility, and resolve can be bolstered by the fact that certain RMA strategies hold the promise of reducing casualties, especially when objectives are kept limited. The RMA can thus be seen to bolster the credibility of deterrent threats because the reluctance associated with carrying out deterrent threats evaporates when the potential costs to the party making good on the threat are minimal. Moreover, because retaliatory strategies that rely on RMA technologies are far less controversial than nuclear retaliation or the deployment of ground forces, RMA- based threats would probably appear more credible to policy makers. There are fewer political restraints on policy makers when they contemplate the use of forces that rely on the RMA".* (FORTMANN; VON HLATKY, 2009, p. 309)

Libicki (2018) dialoga com diversas dessas ideias iniciais de Morgan e Fortmann e Von Hlatky acerca dos efeitos das novas tecnologias para a dissuasão. Para Libicki, adicionar opções intermediárias ao leque dissuasório pode implicar a redução da capacidade dissuasória. Isto aconteceria porque a nova opção de retaliação implicaria em uma punição potencial menor. Quando adicionado a fatores políticos, um dos efeitos provocados é o de que a nova punição poderia ter uma aceitação melhor por parte dos cidadãos em uma democracia. Portanto, uma punição maior e mais adequada poderia ser mais difícil de ser empregada no lugar de uma punição mais leve, potencialmente mais barata e menos letal, mas ao mesmo tempo, menos eficaz.

Com os desenvolvimentos recentes a hipótese de 2003 de Morgan parece estar obsoleta, já que a dominação da defesa parece estar cada vez mais distante. Ataques cibernéticos são mais fáceis de serem perpetrados do que defendidos. A própria ideia de que Estados menores não possam se beneficiar da RMA também deve ser rediscutida; por exemplo, o ataque à Sony, realizado pela Coréia do Norte em 2014[32], foi sofisticado e revelou capacidade cibernética razoável para um país com menos recursos do que o país em que seu alvo se encontrava. Outras tecnologias, como veículos aéreos não tripulados e satélites, também tiveram seus custos massivamente reduzidos. Desta forma, tecnologias continuam a

[32] THE NEW YORK TIMES. **The World Once Laughed at North Korean Cyberpower. No More**. Disponível em <https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html> acesso em 14.nov.2021.

ser desenvolvidas e Estados menores terão dificuldade em estar à frente em seu desenvolvimento, mas, cada vez mais, será difícil negar aos países os benefícios das tecnologias recentes, defasadas em poucos anos ou até meses.

1.2.2. Dissuasão e armas cibernéticas

A possibilidade de ataques devastadores utilizando redes de computadores alcançou a percepção do público em geral em 1983, com o lançamento do filme Wargames, em que um acesso remoto a um sistema de controle de armas nucleares seria capaz de causar a próxima guerra mundial. Poderia ser apenas um filme exagerando nas possibilidades. Entretanto, Ronald Regan, assustado com a perspectiva, perguntou aos seus assessores se aquilo poderia acontecer e eles lhe responderam que de fato algo similar era possível. (KAPLAN, 2017)

Desde então, diversos analistas se debruçaram sobre a possibilidade desse tipo de ataque, e após comprovada a possibilidade, sobre suas potenciais consequências. Após os anos iniciais de especulação, com a internet se tornando ubíqua nos anos 90, os ataques de fato começaram, ainda que em escalas pequenas e com impactos pouco significativos, talvez por conta da inabilidade dos Estados em se adaptarem ou talvez por medo das consequências ou da eventual escalada de qualquer conflito. Inicialmente, a dissuasão no campo cibernético não foi sequer cogitada ou estudada, e suas menções em documentos de defesa foram esparsas (feitas por analogia aos sistemas de informação anteriores) ou inexistentes.

Com os primeiros ataques substanciais no final da década de 1990 e os primeiros problemas de larga escala advindos da ampla difusão de sistemas e redes de computadores, como o *bug* do milênio[33], os analistas começaram a estudar as possibilidades e consequências de ataques e guerras cibernéticas. Nas ciências humanas, o fenômeno representado pela internet ainda era largamente visto como algo positivo (ver, por exemplo, a visão de Castells (2001)) e como fator ampliador das capacidades democráticas e dos direitos humanos. Entretanto, nas ciências militares, o surgimento da interconectividade entre as nações nesta escala e a dependência para com sistemas modernos e redes gerou preocupação. Assim,

[33] O *bug* do milênio se tratava do impacto que a virada de 1999 para 2000 poderia acontecer nos sistemas informáticos mais antigos ainda em operação, pois, nesses sistemas antigos, o ano era guardado com apenas dois dígitos, o que implicaria que em vez de 2000 o sistema interpretaria a virada como 1900. Em sistemas bancários isso poderia gerar juros negativos. No final das contas isso não se demonstrou como um problema, pois os programadores já estavam cientes disso há tempo suficiente para modificar os sistemas. Porém, é interessante notar como a mídia na época aumentou significativamente a atenção do público ao problema, e, por extensão, aos "perigos" da dependência da sociedade nos sistemas informatizados.

alguns analistas passaram a analisar quais os efeitos dessa interdependência em relação às possibilidades de dissuasão nuclear.

1.2.3. Duas Perspectivas

Dissuasão e armas cibernéticas podem ser analisadas sob modos distintos. Nesta tese, argumenta-se duas perspectivas primordiais de análise. A primeira consiste em considerá-las como objetos ou como *fenômeno a ser dissuadido*, colocando-se a pergunta: "como dissuadir um inimigo do emprego de armas cibernéticas *para* empreender um ataque ou *em* um ataque?". A segunda implica considerá-las como novas ferramentas a serem empregadas em conjunto com outros instrumentos dissuasórios já existentes, ou seja, *algo a ser usado para dissuadir*. A pergunta para este caso seria então: "como incorporar as armas cibernéticas ao leque existente de recursos dissuasórios de um determinado Estado? E como isto altera o cálculo dissuasório?"

Tais perspectivas são diferentes e complementares. Portanto, cabe a análise em separado antes de serem entendidas em conjunto nos próximos capítulos. A primeira abordagem entende o domínio cibernético como fator de ameaça e instabilidade, enquanto a segunda como novo instrumental. Argumenta-se, posteriormente nesta tese, que a segunda abordagem é mais importante por oferecer maiores insumos para a compreensão do tema e para a construção de posturas dos principais atores.

Nesta sessão serão brevemente analisadas ambas as perspectivas, os problemas que guiaram as análises e alguns dos entendimentos mais recentes do tema. Nos próximos capítulos as perspectivas serão resgatadas para a análise dos casos apresentados e do caso do vírus Stuxnet e para a compreensão da evolução histórica das possibilidades de ataques e guerra no campo cibernético.

1.2.4. Primeira Abordagem

A primeira abordagem acerca do fenômeno concebe o emprego de armas cibernéticas como *algo a ser dissuadido*. Diversos estudiosos analisaram esse tema, identificando variados fatores recorrentes. Além disso, são identificados argumentos concorrentes, ou seja, a favor da possibilidade da dissuasão e contrários à mesma. As próximas seções serão dedicadas a três

opções analíticas decorrentes: a impossibilidade de dissuadir, a possibilidade de dissuadir (como nos paradigmas anteriores de dissuasão) e alternativa à dissuasão tradicional.

Uma lista, não exaustiva, de fatores é recorrente nessa literatura com o foco em entender o fenômeno como algo a ser dissuadido: 1- problema da atribuição e anonimidade; 2- custos de desenvolvimento; 3- motivação para o uso; 4- discriminação dos alvos a serem atacados (civis contra militares); 5- participação de atores não-estatais; e, 6- possibilidades de escalada não intencional dos conflitos.

Esses fatores surgem com variados graus de importância entre os estudiosos do assunto. A comparação com a dissuasão nuclear pode ser feita com cada fator, e frequentemente as lições mais antigas podem ser utilizadas como analogias aos fenômenos mais recentes. Entretanto, é importante notar que cada fator, mesmo os mais similares, são passíveis de serem modificados pelo advento de novas tecnologias.

1.2.4.1. Impossibilidade de dissuasão

Alguns autores argumentam pela impossibilidade total ou significativa da dissuasão no campo cibernético. O argumento em geral passa pelas características específicas do espaço cibernético e pela dificuldade em se traçar paralelos com os domínios tradicionais de guerra (ar, mar, terra e espaço).

Fischerkeller e Harknett (2017) argumentam que o ciberespaço é um "espaço perpetuamente disputado" e que a dissuasão procura eliminar atividades não desejadas em um ambiente de constante atividade. Trata-se, portanto, de um conceito que não pode ser aplicado[34]. Para os autores, o espaço cibernético possui características únicas, como o baixo custo de entrada, a falta de soberania[35], e a maleabilidade com que ataques podem ser

[34] "(...) Cyberspace is a perpetually contested space. (…) Deterrence applied to cyberspace seeks the absence of unwanted activity in an environment of constant activity and, thus, is a comprehensive mismatch." (FISCHERKELLER; HARKNETT, 2017, p. 386) Entretanto, a concepção de dissuasão como ausência de atividades não desejadas é uma simplificação das diversas possibilidades de dissuasão, como a dissuasão cumulativa de Tor (2015), mesmo em se tratando de dissuasão tradicional. O termo *contested* em inglês será traduzido como *disputado*, em vez de contestado, visando dar um significado mais próximo ao original do autor.

[35]Demchak e Dombrowski (2014) acreditam na possibilidade de soberania no ciberespaço, sugerindo redes de internet separadas para cada país. A posição destes autores revela uma incompreensão profunda sobre como a rede funciona, pois os protocolos foram definidos exatamente para tornarem possível passar por este tipo de bloqueio, mesmo com dificuldades, o que é bem demonstrado pelas diversas maneiras de burlar o bloqueio e a censura de sites praticada pela China (também conhecido como *Great Firewall of China*), mesmo com custos técnicos altos. O controle total da rede, com a desconexão do restante do mundo, traria consequências econômicas desastrosas para qualquer país desenvolvido que tentasse isso. (Para uma discussão sobre o controle governamental da internet ver Wives (2013)) O exemplo da Coréia do Norte demonstra que mesmo para um país extremamente fechado a internet é importante, e é utilizada pelas elites e até como ferramenta de ataque, como

empregados (em termos de tamanho e escopo dos danos possíveis), assim como as dificuldades inerentes de atribuição. A argumentação dos autores pela impossibilidade de dissuasão é de que as políticas para o domínio não levam em consideração estes fatores.

Comparar a soberania no espaço cibernético com a soberania tradicional é um exercício sem saída analítica possível. Embora a nomenclatura de "espaço" possa parecer comparável com "território", as conceituações são de naturezas diferentes. Não é possível comparar o espaço virtual ao real esperando que sejam possíveis a criação de barreiras, fronteiras, controles de passaporte, ou outras características aplicadas ao deslocamento de pessoas e bens entre países. Chamar a rede mundial de computadores de "espaço cibernético" é uma analogia útil para a compreensão das possibilidades da rede, mas o argumento de Fischerkeller e Harknett (2017) e de Demchak e Dombrowski (2014) entende o espaço cibernético como *território* e passível dos mesmos controles, levando a uma extrapolação errônea dos termos.

O argumento de que o custo de entrada é baixo, permitindo a atuação de atores individuais, não parece se sustentar no nível de análise proposto para a compreensão dos fenômenos de dissuasão cibernética. Os ataques impactantes após o início dos anos 2000 foram de grande sofisticação, requerendo recursos monetários e não monetários que indivíduos dificilmente poderiam levantar sozinhos. Por outro lado, certas ações perpetradas por atores não estatais podem ter impactos significativos para as relações internacionais mesmo fora do ambiente cibernético, como no caso dos ataques de 11 de setembro de 2001. A incapacidade de dissuadir ataques terroristas de larga escala não modifica, a princípio, a relação de dissuasão entre os países. Da mesma maneira, a incapacidade de dissuadir ataques realizados por atores não estatais no espaço cibernético não deveria impedir a dissuasão entre os países nesse domínio.

O domínio cibernético é criado pelo homem e é dinâmico, ao contrário dos outros domínios tradicionais (terra, ar, água) onde os combates desdobram com planos de fundo estáticos (KELLO, 2017). Esta característica complica as ações no meio, pois o meio não é apenas o veículo, mas pode ser ele próprio modificado pelas ações dos atores. O fato do meio ser disputado, como argumentam Fischerkeller e Harknett (2017), não modifica o fato de que

---

no caso dos ataques contra a Sony em 2014 (e no caso da Coréia do Norte, também é utilizada como fonte de captação de recursos pelo governo, por meio de crimes econômicos cibernéticos patrocinados pelo Estado (ver a reportagem da Reuters: *"North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report"* disponível em: <https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX> acesso em 08.ago.2020)).

os atores detentores de capacidade operativa de fato, ou seja, os Estados, possuem motivações e objetivos comparáveis, independentemente do domínio em que operam. Não há objetivos estratégicos fundamentalmente diferentes em ações de guerra em domínios diferentes, e as diferenças entre os objetivos táticos ou operacionais de cada meio não são relevantes para o nível de análise que abarca as questões de dissuasão entre os países[36]. Portanto, não faz sentido aceitar a impossibilidade de dissuasão, a não ser que essa impossibilidade também se estenda aos outros domínios.

Além disso, conceitos da abordagem tradicional de dissuasão, como dissuasão por negação e dissuasão por punição, são frequentemente aplicados às operações de Estados no meio cibernético. As ações técnicas que protegem os sistemas são facilmente comparáveis às técnicas de dissuasão por negação, e as doutrinas de defesa militar de alguns países (e.g: EUA e o Reino Unido, como demonstrado anteriormente) encaram a dissuasão por punição como possível de ser aplicada no campo cibernético. Então, mesmo que a dissuasão não fosse possível, os Estados ainda a veriam como minimamente possível e estariam tentando praticá-la, com variados graus de sucesso ou insucesso.

1.2.4.2.Possibilidade da Dissuasão

Ao se analisar o campo cibernético como passível de ser dissuadido é necessário entender: 1- se essa dissuasão se dará em termos similares aos da dissuasão nos outros domínios ou; 2- se ela se demonstrará de uma nova maneira. Para a primeira abordagem é necessário assumir que os impactos e as estratégias são similares aos domínios tradicionais. Para a segunda, é necessário entender como as peculiaridades específicas do domínio impactam a dissuasão e a maneira em que ela se demonstra.

Brantly (2018) argumenta que a dissuasão é possível no meio cibernético, mas que a dissuasão, seja por punição ou negação, sozinha, não é suficiente e necessita ser combinada com outras estratégias para ser eficaz. Para ele, a dissuasão cumulativa pode ser uma dessas estratégias, mas também não é suficiente, e o resultado final esperado deve ser a dissuasão no sentido tradicional de se evitar ataques (e não de apenas reduzir a magnitude ou o impacto deles).

[36] Por exemplo, as ações da Rússia em relação à Geórgia, Ucrânia e Estônia desde 2007 podem ser entendidas, nos níveis político e estratégico como a tentativa de uma nova consolidação da esfera de influência russa em territórios anteriormente participantes da União Soviética. A utilização de armas cibernéticas ou de invasões terrestres vai ter resultados diferentes e impactos de magnitudes diferentes, mas, neste exemplo de análise, o objetivo estratégico ou político está desconectado do domínio onde a operação ocorre e, portanto, não muda.

Brantly apresenta o caso do *Solar Sunrise*[37] como exemplo da dificuldade de se dissuadir ao lidar com atores não estatais, e como a atribuição de um ataque interno a um outro Estado demonstra os riscos da atribuição errônea. Para ele, o contexto estratégico e operacional em que os atores agem pode levar à compreensão de como lidar com o problema da atribuição, para cada caso, embora apenas o entendimento destes contextos, sem outras análises, dificilmente seria suficiente.

A dissuasão tradicional pode se demonstrar pela quantidade reduzida de ataques de larga escala e impacto nos últimos anos. Se a definição de ataques cibernéticos passíveis de serem dissuadidos incluir apenas os ataques com resultados similares a ataques cinéticos com destruição física de ativos (ataques da categoria *sabotagem*) a quantidade de ataques entre Estados após o vírus Stuxnet no Irã foi praticamente zero[38]. Entretanto, há de se notar que danos econômicos similares a ataques tradicionais foram de fato verificados em diversas ações cibernéticas posteriores.

Applegate (2013) discorre sobre as possibilidades iminentes de danos equivalentes a ataques cinéticos substantivos serem causados por armas cibernéticas, com evidências experimentais de diversos casos e possibilidades de uso[39]. O autor argumenta que a utilização do vírus Stuxnet levaria a uma legitimação do uso de capacidades cibernéticas com danos similares a ataques cinéticos. Entretanto, a despeito das grandes possibilidades e de evidências de seu uso razoavelmente bem-sucedido no Irã, os ataques desta natureza não são comuns. De alguma maneira, algum tipo de efeito dissuasório parece estar em curso, seja algo difuso, como o medo da escalada de conflitos, ou algo específico, como as doutrinas de retaliação a ataques cibernéticos expressas em documentos de defesa das grandes potências.

1.2.4.3.Alternativa à dissuasão tradicional

Tor (2015) analisa como a dissuasão cumulativa, aos moldes da dissuasão israelense, poderia ser aplicada ao ciberespaço. Para ele, a questão foi erroneamente analisada sobre os moldes da dissuasão nuclear. Pois, no domínio cibernético, a dissuasão por retaliação/punição

[37] Dois hackers americanos e um israelense invadiram mais de 500 sites do governo norte-americano, incluindo sites do exército. Inicialmente a suspeita recaiu sob uma ação de hackers iraquianos. Ver capítulo 2 para uma discussão sobre este caso.

[38] Em outros ataques de sabotagem identificados a destruição de ativos se deu de maneira indireta. Pode-se argumentar que a Ucrânia tenha sofrido uma sabotagem comparável ao Irã, isso será discutido no próximo capítulo.

[39] Para uma linha do tempo com diversos incidentes cibernéticos com resultados cinéticos ver: <https://ivezic.com/timeline-cyber-kinetic-attacks-incidents/> acesso em 10.out.2019.

e a dissuasão por negação não são estratégias críveis, porque tentam aplicar conceitos que não seriam facilmente transportados, como a destruição mútua assegurada e outros.

A dissuasão por retaliação/punição envolve a garantia de uma resposta com o mesmo valor punitivo ou maior que o ataque. Entretanto, uma das questões levantadas seria: como retaliar no espaço cibernético ativos de valor similar? ; ou ainda, como justificar um ataque tradicional se o dano causado não for necessariamente físico? O problema da atribuição e da consequente negação plausível torna a punição mais problemática. Há um risco em se punir um ator que não tenha cometido o ataque. Ainda mais, um terceiro ator pode tentar começar um conflito ao mascarar a atribuição de um ataque. Qual seria o limiar razoável de certeza de atribuição para um ataque retaliatório? 99%? 99,99%? E se o potencial alvo da retaliação for uma potência nuclear? Qual seria o caminho de ação mais adequado? Uma resposta econômica e diplomática poderia ser encarada como uma incapacidade dissuasória, caso o ataque envolva ganhos claramente militares.

A dissuasão por negação, neste caso, é muito similar a estratégias defensivas. Implica limitar os potenciais ganhos de um adversário em caso de ataque, tornando as defesas difíceis de serem penetradas, ou tornando pouco relevantes as consequências da agressão. Neste campo, entra a questão da resiliência. Sistemas que possam ser rapidamente restaurados após um ataque e rapidamente reforçados para resistir a ataques similares podem reduzir consideravelmente os ganhos de um agressor. No ciberespaço, a defesa é consideravelmente mais cara que o ataque (NYE, 2017). Portanto, garantir a resiliência pode ser uma estratégia mais exitosa em termos de dissuadir ataques pela possibilidade de negação dos benefícios aos agressores[40].

Ataques de naturezas diferentes requerem estratégias dissuasórias diferentes. Os principais ataques podem ser categorizados como sendo de *subversão*, *sabotagem* e *espionagem*[41]. Os ataques de sabotagem possuem potencial de infligirem danos físicos com ações no ciberespaço. Portanto, são frequentemente os casos analisados em situações de dissuasão. A subversão pode minar as estruturas democráticas e burocráticas de um país, mas requer um modelo de dissuasão diferente, pois pode ser conduzida de maneira não militar, e

[40] "(…) Cyber defenses are notoriously porous, and the conventional wisdom holds that offense dominates defense. Good cyber defenses, however, can build resilience or the capacity to recover, which is worthy in itself; they can also reduce the incentive for some attacks by making them look futile. (…). Resilience is essential both to reduce an adversary's benefits of attacking critical infrastructure and to assure that cyber and noncyber military response options are available for retaliation." (NYE, 2017, p.56)

[41] "(…) while cyber OAAs vary significantly, it is important to think through three categories discussed in academic analysis and policy circles- sabotage, espionage, and subversion." (FISCHERKELLER; HARKNETT, 2017, p.383)

com grandes possibilidades de negação plausível. As ações cibernéticas associadas à espionagem podem ser estudadas analogamente às ações tradicionais de espionagem. Impedir a ação de espiões é algo tentado desde os primórdios das guerras e a adição do elemento cibernético não parece mudar significativamente este panorama.

Ao se analisar ataques cibernéticos como *fenômeno a ser dissuadido*, entende-se, portanto, que a maioria dos casos correspondem a ações categorizadas como *sabotagem*[42]. A análise de Tor (2015) leva em consideração este tipo de ataque, embora seja argumentado nesta tese que os outros tipos de ações também sejam passiveis de serem dissuadidas dentro desta perspectiva. Para o autor, a dissuasão cumulativa implica um jogo repetido diversas vezes. O objetivo não é evitar a totalidade dos ataques, mas definir as regras do jogo, de modo a que os ataques tenham menor impacto e sejam cada vez mais esparsos ao longo do tempo. Neste sentido, a ocorrência do ataque não seria, em si mesma, uma falha da dissuasão, mas deveria ser analisada em seu contexto, com as possíveis seguintes perguntas: 1- Este ataque poderia ter sido maior e foi limitado em seu escopo? ; 2 – Como utilizar deste ataque para demonstrar capacidades de maneira dissuasória? Caso o ataque tenha sido mais limitado que o previsto, a estratégia de dissuasão cumulativa teria funcionado. Em qualquer resposta, a segunda pergunta encara o ataque como oportunidade de testar as regras do jogo que foram definidas até então e de definir as regras para as próximas rodadas.

Tor (2015) resume a abordagem da seguinte maneira:

> *"(...) Applied to the cyber domain, the cumulative deterrence paradigm does not unrealistically seek to prevent cyber-attacks from ever occurring. Instead, it takes for granted the inevitability of some acts of cyber aggression and strives to shape and limit them by attacking the rival repeatedly in response to specific behaviors, over a long period of time, sometimes even disproportionally to its aggressive actions*". (TOR, 2017, p. 95)

Para utilizar uma estratégia de dissuasão cumulativa um Estado, segundo Tor (2015), deve-se responder cada ataque, mesmo que de maneira desproporcional, em uma perspectiva de aprendizado contínuo entre os atores com múltiplas iterações[43]. Como já dito, a resposta

[42] Entretanto, como será visto na análise dos casos, mais recentemente, os fenômenos de subversão cada vez mais são alvos de ações dissuasórias. E talvez até essa importância inicial dada aos ataques do tipo sabotagem por muitos analistas possa ter aberto o espaço para as ações massivas de subversão vistas nas eleições estadunidenses.

[43] Pode-se argumentar que, dentro da Teoria dos Jogos, a dissuasão cumulativa possa ser entendida como um jogo repetido, e além das opções disponíveis para os participantes em cada etapa é entendido o fenômeno da aprendizagem mútua e os limiares de agressão definidos se tratam de momentos em que a retaliação aumentaria em intensidade. Esses limiares não são o ponto sem retorno, como no modelo de *brinkmanship* de Powell(1990). A estratégia de "olho por olho, dente por dente" (*tit-for-tat* em inglês) estabelecida na teoria dos jogos encara, de certa maneira, esse fenômeno de aprendizagem, pois consiste em uma resposta na mesma medida, começando

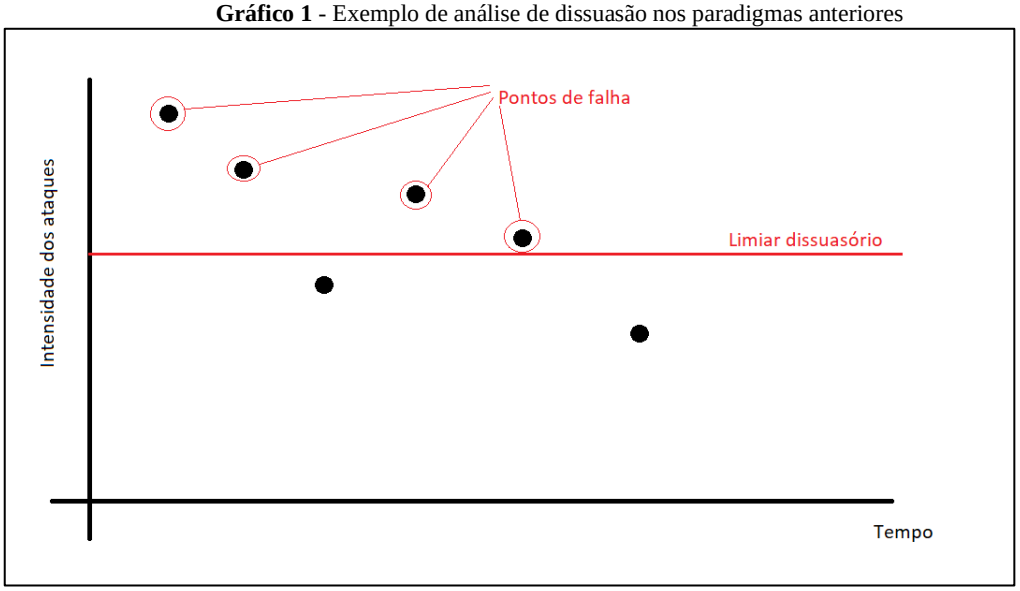
não deve necessariamente ter o objetivo de impedir completamente ataques futuros, mas delimitar os limiares a que um agressor pode chegar antes de receber uma resposta. A dissuasão, neste sentido, seria gradual, com o comportamento dos agressores sendo moderado ao longo do tempo, em vez de completamente interrompido. Neste caso, a dissuasão é complementada por ações que visem compelir (*compellence*) um Estado a agir de determinada maneira, mesmo que o objetivo final seja evitar, ao máximo, as ações agressivas. Cada troca entre os atores é um ponto de aprendizado dentro da relação de rivalidade.

Em resumo, segundo Tor:

> *"The theory is that multiple victories accumulated by the deterring party over extended periods of time through the duration of the conflict ('the game') will gradually produce more moderate behavior ('rules of the game') on the part of the adversaries".* (TOR, 2015, p. 108)

Nos gráficos abaixo são delineados exemplos da diferença de análise em relação aos paradigmas de dissuasão. Cada ponto nos gráficos representa um ataque sofrido. Em termos de dissuasão tradicional, no primeiro gráfico, as ações acima de um determinado "limiar dissuasório" - um limite onde uma ação agressiva seria considerada não aceitável - são consideradas falhas na capacidade dissuasória de um país.

Gráfico 1 - Exemplo de análise de dissuasão nos paradigmas anteriores

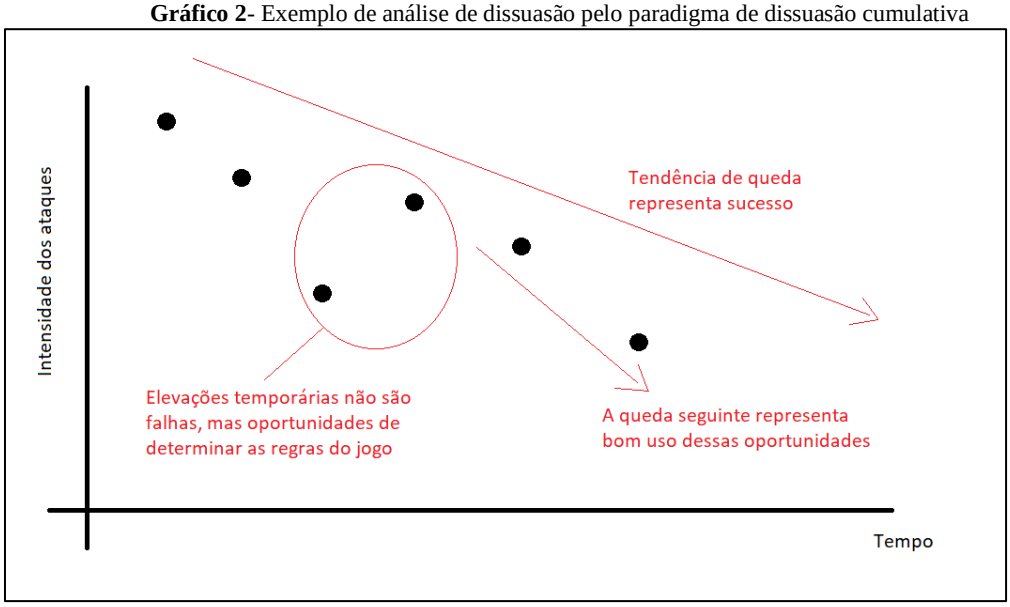


Fonte: Elaborado pelo autor (2021)

com a cooperação e punindo a ausência dela pelo outro ator. Neste caso, a análise precisa ir além das escolhas entre cooperar ou não cooperar, pois a ideia de diminuição de intensidade de ações agressivas dentro de cada iteração é considerada como um sucesso (entendendo então *graus* de cooperação e não cooperação). Dentro da análise do dilema do prisioneiro repetido isso pode fazer sentido, porém o cálculo dissuasório a ser realizado pelos Estados é necessariamente mais complexo do que esse dilema, e para uma compreensão dos processos decisórios práticos de um país é necessário ainda analisar outras questões, como os aspectos culturais dos atores envolvidos e as peculiaridades dos domínios (como as questões abordadas de soberania e atribuição no domínio cibernético).

O segundo gráfico representa os mesmos pontos de ataques ao longo do tempo, entretanto, em uma análise baseada no paradigma da dissuasão cumulativa, a diminuição da intensidade das ações ao longo do tempo representa-se o sucesso, e cada ataque retaliado à altura pode determinar as regras de engajamento futuras. A análise não deve ser feita ponto a ponto, mas a partir da tendência geral do gráfico.

Gráfico 2- Exemplo de análise de dissuasão pelo paradigma de dissuasão cumulativa



Fonte: Elaborado pelo autor com base em Tor (2015)

Entretanto, é possível criticar esta abordagem em determinadas circunstâncias. O primeiro ponto de crítica é a identificação correta dos agressores, ou seja, o problema da atribuição. Segundo Tor (2015)[44] e Iasiello (2013)[45], isso não é necessariamente um problema, pois a atribuição pode ser feita segundo capacidades operacionais e estratégicas dos potenciais agressores. Porém, pode-se argumentar que, ainda assim, a negação plausível poderia impedir o Estado defensor de agir mesmo em situações com baixa incerteza.

O cálculo de dissuasão nuclear entra em consideração quando o potencial agressor possui armas atômicas, ou é um aliado importante de uma das potências nucleares. Ações de dissuasão cumulativa, todavia, não parecem ter sido aplicadas durante a Guerra Fria, o que leva a crer que entre grandes potências, ela não seria factível. Israel possui adversários imediatos que, embora tenham o desejo, não possuem a capacidade de destruição total e

[44] "The romantic idea of anonymity in cyberspace does not hold when dealing with nation-state actors, due to both the *strategic context* and the *operational reality* of these actors' behavior" (TOR, 2015, p.9 grifo no original)

[45] "(...) While attribution in cyberspace is nearly impossible, certain elements such as actor motivation, intent, behavioral actions, actor profiling can be identified, evaluated, and assessed to help better understand the significance of these cyber events – not just from an operational level, but from a strategic perspective as well." (IASIELLO, 2013, p.454)

completa. Assim, faz sentido que um conflito possa ser respondido com força desproporcional, uma vez que não há o perigo imediato de uma escalada catastrófica do confronto, pois se entende que ele já está no nível que o agressor deseja. Como estudado na questão da dissuasão durante a Guerra Fria, o cálculo das grandes potências deve ser diferente, pois implica possibilidades de danos mais profundos em degraus mais altos da escada dos conflitos, inatingíveis por atores não nucleares.

Outro problema gerado pela análise a partir do paradigma da dissuasão cumulativa é entender os acontecimentos conforme eles se desdobram. No exemplo de análise sob o paradigma de dissuasão cumulativa fornecido anteriormente, ao se analisar a linha do tempo como um todo é fácil perceber o sucesso dissuasório. Entretanto, ao se vivenciar cada ponto, as elevações temporárias podem aparentar ser, naquele momento, uma falha da dissuasão, muito embora em prazos maiores e em uma análise posterior, não o sejam. Portanto, a abordagem requer um entendimento mais holístico por parte dos tomadores de decisão, principalmente em termos temporais, bem como o entendimento de que raramente a intensidade dos ataques vai decrescer de forma regular e sustentada.

Além disso, as questões de diferenças culturais podem ser analisadas em termos da aprendizagem entre os atores. As diferenças de definições e entendimentos podem gerar ruídos na comunicação, impedindo a transmissão clara de mensagens dissuasórias, ainda mais ao se tratar de ações rápidas com tempos limitados de resposta.

Por fim, é razoável argumentar que a capacidade dissuasória de Israel comportou falhas, mesmo em uma perspectiva de análise de longo prazo. Não se espera que a dissuasão cumulativa seja uma solução sem falhas para o campo cibernético, mas sim uma solução mais factível e sustentável do que os entendimentos anteriores.

A análise do paradigma de dissuasão será feita, nesta tese, a partir dos estudos dos casos apresentados. Neles, serão identificados os elementos que poderiam ter sido compreendidos dentro do paradigma de dissuasão cumulativa pelos atores, e quando possível, as potenciais consequências da não utilização de oportunidades de aprendizado ou outras ações dentro deste paradigma. Em adição, é possível identificar, em casos importantes, múltiplas iterações entre os atores, possibilitando a análise de aprendizados e as regras do jogo delimitadas entre eles, como no caso da Ucrânia e até mesmo no Stuxnet. Os aprendizados podem ser analisados alternadamente pelo ponto de vista dos atores envolvidos. No caso da Ucrânia, será demonstrado como o aprendizado do agressor possibilitou a

escalada das ações. No caso do Stuxnet, a ambiguidade sobre os papéis de agressor e defensor será explicitada, e como isso pode ter alterado os cálculos e as percepções acerca dos limiares dissuasórios envolvidos.

Pela natureza de longo prazo de sua aplicação, o paradigma deve ser validado com análises em prazos maiores. Casos concisos possuem menos elementos que determinem a utilidade da abordagem, enquanto casos mais longos podem ter seus aspectos de aprendizagem e de trocas entre os atores melhor caracterizados. Ainda assim, casos menores podem fornecer indícios em atuações mais amplas das estratégias de defesa e dissuasão dos países.

A inadequação do paradigma poderia ser demonstrada, caso o aspecto de aprendizagem entre os atores não seja identificado. Nesta possibilidade, as análises sobre adequação do conceito de dissuasão no domínio cibernético teriam de ser retomadas, sob os moldes das teorias tradicionais de dissuasão. Demonstrar-se-á que este paradigma aparenta ser adequado, porque os aspectos de iteração e aprendizado são presentes mesmo quando as estratégias utilizadas pelos países alvo de agressões não tenham sido construídas sob este paradigma. Além disso, serão identificados diversos momentos em que a inação, ou baixa proporcionalidade das respostas, resultou em consequências, demonstrando o aprendizado do ponto de vista do agressor e apontando uma continuidade de ações agressivas ao longo do tempo.

1.2.5. Segunda abordagem: adição ao leque dissuasório

A segunda abordagem a ser analisada entende que o domínio cibernético e suas armas são *adições* às capacidades dissuasórias de um Estado. Neste sentido, o emprego de armas cibernéticas complementa as possibilidades de dissuasão nuclear e não-nuclear. O ciberespaço é entendido como um campo de batalha, não importando se os ataques se restringem a ele ou se provocam danos em outros domínios. O que importa, ao final, são as possibilidades conjuntas, dentro do leque de opções de que cada país dispõe.

Os elementos apresentados, no caso do vírus Stuxnet no capítulo 3, serão analisados à luz dessa abordagem. A análise do caso permitirá verificar os efeitos dissuasórios dentro do leque de possibilidades que os EUA e Israel possuíam nos períodos imediatamente anteriores e posteriores ao ataque.

Não obstante qualquer evolução do tema, a adição de armas cibernéticas ao leque dissuasório dos Estados poderá ser facilmente verificada e estudada nas próximas décadas. Uma análise futura com os documentos de defesa dos países e os relatos de seu emprego poderão ser insumos para outro estudo. Os argumentos presentes nesta tese poderão ser corroborados ou falseados dependendo da evolução futura do tema.

1.2.5.1.Pressupostos

Um dos pressupostos iniciais desta abordagem é que, qualitativamente, os potenciais danos de armas cibernéticas são similares às opções de respostas e ações tradicionais, principalmente: retaliações econômicas, diplomáticas ou retaliações com armas cinéticas. Um Estado que possa ser dissuadido com as ferramentas tradicionais poderia, portanto, ser dissuadido com armas cibernéticas, e o cálculo dissuasório seria similar. A questão quantitativa, ou seja, a extensão do dano, pode potencialmente ser estimada[46].

Um país que não utilize novas tecnologias estaria teoricamente imune a um ataque cibernético. Entretanto, os custos de não utilizar tecnologias modernas são muito elevados. Portanto, mesmo as nações mais isoladas estão também vulneráveis e poderiam ser dissuadidas segundo esta abordagem.

Um Estado que deseje adicionar capacidades cibernéticas ao seu leque de opções dissuasórias deve possuir capacidades técnicas (principalmente em termos de recursos humanos) aliadas ao desenvolvimento constante de tecnologias. Mesmo as armas nucleares requerem manutenção constante, pois o material físsil decai naturalmente e os sistemas de localização de alvos e segurança podem degradar com o tempo. Com armas cibernéticas não é diferente, mas os ciclos de desenvolvimento e manutenção devem ser mais curtos, já que eventuais vulnerabilidades podem ser rapidamente corrigidas pelos fabricantes de software ou abertamente divulgadas por pesquisadores da área possibilitando a construção de defesas. Capacidades técnicas suficientes permitem a criação e a manutenção de um arsenal variado de armas cibernéticas que podem ser empregadas rapidamente quando convier, sendo ao mesmo

[46] É interessante o paralelo com armas nucleares modernas que podem ter o seu poder explosivo modificado com a virada de um botão (*dial-a-yield*), isto pode ter possibilitado em parte a redução dos arsenais nucleares, pois uma mesma arma pode suprir mais de um papel estratégico/tático. A calibração do poder de armas cibernéticas poderia reduzir os custos de manutenção e desenvolvimento, pois, da mesma maneira, uma mesma arma pode ter mais de um papel. Entretanto, neste caso, a arma estaria mais suscetível a ser tornada obsoleta pelo conserto de uma vulnerabilidade (um *patch*), de qualquer modo a capacidade técnica dos grupos que a desenvolveram permanece, e pode ser aplicada em futuros desenvolvimentos.

tempo, resilientes à correção de vulnerabilidades dos softwares, pela variedade de vetores de ataque possíveis de serem utilizados.

Não é necessário argumentar que os sistemas informatizados sempre serão suscetíveis a vulnerabilidades. Com o aumento da complexidade dos sistemas cibernéticos, uma defesa eficaz fica cada vez mais distante. O argumento de que o desenvolvimento de capacidades defensivas de natureza cibernética seria suficiente para impedir ataques de mesma natureza não parece se sustentar. Em adição, operações de subversão são passíveis de emprego mesmo frente a sistemas que fossem razoavelmente seguros, pois se tratam de campanhas de informação utilizando os próprios canais que perfazem o espaço cibernético.

O último pressuposto é de que os Estados estão dispostos a empregar capacidades cibernéticas com propósitos dissuasórios. O medo da escalada de conflitos, ou de efeitos colaterais indesejados poderia adiar significativamente tal emprego. A não ocorrência de ataques cibernéticos resultantes em destruição física em larga escala, após o vírus Stuxnet, poderia apontar nessa direção. Entretanto, o efeito dissuasório das armas nucleares é inegável, apesar das mesmas não terem sido empregadas após a Segunda Guerra Mundial. Nesse sentido, é possível cogitar que os testes nucleares de larga escala possam ser substituídos por outras formas de demonstração de força e capacidades no domínio cibernético, com ataques sofisticados e públicos, mas contidos, demonstrando a capacidade com riscos mínimos de escalada.

1.2.5.2.Problemas

Segundo Libicki (2018), se compararmos o recurso das opções dissuasórias intermediárias (como por exemplo, a cibernética) à dissuasão nuclear e à destruição mútua assegurada, a credibilidade da ameaça seria comprometida, e assim incentivar-se-ia agressões por parte do ator alvo da dissuasão. Isto ocorre porque uma ação dissuasória intermediária (que envolva punição potencialmente menor) abre a possibilidade do eventual agressor (cujo ataque se deseja dissuadir) aceitar o risco da punição menor, pois lhe caberia estimar a quantidade de punição ser recebida (incentivando-o assim, a perpetrar o ataque, mesmo que fosse com menores potenciais destrutivos ou com menores ganhos estratégicos).

Para Libicki, a ocorrência do ataque corresponde a uma falha da dissuasão, enquanto no paradigma de dissuasão cumulativa, um ataque que é propositadamente moderado pelo

agressor representa um entendimento das regras do jogo e, portanto, um indicativo que a dissuasão está funcionando.

Em qualquer caso, a adição de opções dissuasórias intermediárias pode complicar os cálculos estratégicos dos atores envolvidos. Mesmo formas mais simples de dissuasão requerem comunicações precisas e bem articuladas, para que os potenciais agressores tenham certeza da inevitabilidade da resposta. Em cenários com mais opções, esta incerteza pode se traduzir em falhas dissuasórias, uma vez que intenções mal comunicadas podem ser interpretadas erroneamente pelo suposto agressor, alimentando nele, por exemplo, um otimismo exagerado em relação à própria capacidade de contra resposta ou à capacidade de tolerar a punição. Neste caso, tanto a punição a ser perpetrada, quanto seu caráter iminente devem ser claramente comunicados. Um documento de defesa que explicite apenas que ataques cibernéticos podem ser retaliados não teria efeito sem a definição precisa do que é considerado um ataque cibernético, ou da retaliação que o mesmo suscitará segundo a magnitude de ataque sofrido. Tal definição estratégica não é comum em documentos de defesa, mesmo em outros domínios, mas poderia ser uma ação para o reforço de credibilidade no domínio cibernético, onde as definições de diversos conceitos ainda são imprecisas.

A dissuasão cumulativa parece ser mais útil para um fenômeno que tende a ser contínuo. Uma hipótese plausível é que a inexistência de punições para ações no espaço cibernético tende a tornar o espaço cada vez mais disputado. Ao se considerar que ações de subversão no meio cibernético são difíceis de serem objeto de ações dissuasórias críveis e proporcionais, e frequentemente não serem alvos de respostas temporalmente adequadas (de acordo com o necessário para a dissuasão cumulativa), a frequência e a intensidade dessas ações tenderiam a aumentar com o tempo. Um entendimento de cada ataque como falha dissuasória encara cada ponto como único e extraordinário, em vez de um possível jogo interconectado de agressões e respostas, que pode se seguir após repetidos ataques bem-sucedidos no meio. Portanto, entender cada ataque como oportunidade de definir as regras do jogo parece ser mais útil para compreender como o fenômeno de fato evolui. Ações de sabotagem podem ser consideradas como mais impactantes e mais passíveis de serem retaliadas. Por isso a dissuasão geral contra estas estaria em funcionamento, e por isso os testes dos agressores tenderiam a se concentrar em ações que gerariam retaliações menores e em campos menos impactantes, como o diplomático.

1.3.BALANÇO DA DISCUSSÃO

Desde a concepção inicial da dissuasão militar, passando pela dissuasão nuclear até a entrada das armas cibernéticas no cálculo dissuasório o conceito evoluiu e foi se modificando. A influência de novas tecnologias nos assuntos militares sempre foi uma constante e o advento das armas cibernéticas é mais um passo neste fenômeno. Ainda há relutância por certos autores em admitir a mudança paradigmática em curso. Entretanto, outros estudiosos perceberam desde o início o potencial de mudança das novas tecnologias.

Em termos militares, o emprego de novas tecnologia em geral, analisado inicialmente como "Revolução em Assuntos Militares" (RMA), aparentemente não se deu de maneira repentina e totalmente disruptiva, como o termo "revolução" implicaria. Representou, antes, uma constante evolução desde, pelo menos, os anos 80, como apontado já em 2009 por Fortmann e Von Hlatky. O desenvolvimento e emprego das armas cibernéticas podem ser entendidos como mais um passo nessa "revolução", neste caso, com duração de pouco mais de duas décadas. Porém, em se tratando de emprego em campo, a capacidade de empregos disruptivos de tecnologias cibernéticas é constante, tanto devido às possibilidades de desenvolvimentos encobertas quanto à utilização rápida. Isso adiciona um elemento duplo à análise; por um lado, desenvolvimentos contínuos e constantes, e, por outro, de usos repentinos e impactantes. Esses elementos se relacionam, mas ao mesmo tempo também distanciam a análise das armas cibernéticas da análise inicial da RMA.

A escolha metodológica em dividir a análise em duas perspectivas ou abordagens, como a adição ao leque dissuasório ou ser sujeito à dissuasão dentro do novo domínio, pode ser transitória. Esse é um artifício analítico derivado da necessidade de se tentar entender um fenômeno em evolução e enquanto o próprio analista é participante. Entretanto, espera-se que o valor e o sentido dessa escolha fiquem claros nos próximos capítulos em que a moldura de análise será aposta aos casos mais interessantes de conflitos no ciberespaço, do ponto de vista das relações internacionais.

Os caminhos que os estudos acerca da dissuasão trilharão e aonde chegarão nos próximos anos podem apenas ser objeto de conjectura no presente. A análise da segurança entre os países molda e é moldada pela capacidade dos analistas e teóricos em entender eventos que se desdobram em comparação com eventos anteriores. As tecnologias disruptivas

abalam esta capacidade, pois os critérios e pontos de comparação se alteram no tempo. Pode-se argumentar que as armas cibernéticas podem ser analisadas sob o prisma das mais recentes abordagens militares. É possível, entretanto, que o efetivo emprego das armas cibernéticas não ofereça ainda lastro suficiente ao estudo avançado das mesmas e de sua miríade de implicações. Portanto, o campo ainda pode sofrer alterações bruscas e repentinas.

Eventos do tipo *black swan*, os quais desafiam a lógica corrente, podem ter impactos significativos sobre o desdobramento dos conflitos. A recente epidemia do novo coronavírus provocou uma profunda recessão mundial, com efeitos inesperados nos diferentes âmbitos de interação entre os países, inclusive o militar. Os cálculos dissuasórios e as janelas de oportunidade que se abrem nesses momentos podem precipitar ações antes planejadas para um futuro mais distante ou questionar severamente o padrão de racionalidade de atores-chave envolvidos em questões militares.

Os pressupostos de racionalidade e a própria importância do cálculo dissuasório são fontes constantes de dúvidas. O papel da irracionalidade instrumental e da diferença entre as culturas e valores dos atores envolvidos faz com que modelos generalizáveis sejam difíceis de serem construídos, uma vez que cada caso requer seleção precisa de variáveis, que frequentemente serão únicas. Ainda assim, espera-se recolher lições importantes ao se analisar historicamente a evolução do fenômeno e até mesmo identificar variáveis que confiram certa constância entre os casos.

A alternativa para a questão da própria possibilidade da dissuasão é entender como as armas cibernéticas podem entrar no rol de possibilidades dissuasórias de um Estado. Ameaças representadas por sanções políticas e econômicas e ataques convencionais já são bem compreendidos tanto como degraus da escalada de conflitos como meios de dissuasão não-nuclear. As armas cibernéticas, por sua vez, suscitam novas possibilidades para um Estado que deseje dissuadir, e trazem consigo, ao mesmo tempo, mais "pontos de pressão", isto é, de vulnerabilidades, as quais podem ser exploradas tanto por potenciais agressores quanto por eventuais defensores.

Esta perspectiva permite abordar aspectos de conhecimento relevantes sobre a dissuasão no campo cibernético como forma de relação de poder entre países, tais como as motivações para o recurso a armas cibernéticas em diferentes contextos, as opções dissuasórias de impacto similar, e suas consequências e uma melhor definição do lugar das armas cibernéticas no espectro dissuasório. Portanto, ainda que permaneça aberta a discussão

sobre possibilidade ou não de dissuasão no campo cibernético, o impacto e implicações das tecnologias cibernéticas nos âmbitos da segurança e da defesa a transcendem. Os Estados não abdicaram do emprego de tais armas, e as têm efetivamente empregado, mesmo que com cautela. Seus diversos efeitos, dissuasórios ou não, podem, portanto, ser auferidos analiticamente.

2. HISTÓRICO DE ATAQUES CIBERNÉTICOS

O objetivo deste capítulo é analisar como alguns dos principais ataques cibernéticos (entre Estados) se desenvolveram com base em sua tipificação (sabotagem, subversão e espionagem). Serão também analisadas as respostas dos países envolvidos assim como as reações entre os países acerca do ataque e a questão da atribuição e da soberania. Também será discutido o entendimento dissuasório a ser aplicado ao caso: dissuasão cumulativa, impossibilidade de dissuasão ou possibilidade. Nos casos em que for relevante, uma breve discussão técnica será apresentada no texto ou em notas de rodapé.

Os casos estão organizados em três períodos. O primeiro se refere aos primórdios das operações cibernéticas, até o ano 2000. O segundo se refere à primeira década dos anos 2000 e demonstra o desenvolvimento e a manutenção de atores com grande capacidade de coordenação. O terceiro período são os anos posteriores à descoberta do Stuxnet que marcam a consolidação da sofisticação dos ataques e das capacidades desenvolvidas pelos principais atores.

A análise a seguir é de caráter exploratório no que tange aos elementos a serem empregados na análise do caso do Stuxnet no Irã. O caso do Stuxnet se relaciona com os anteriores e posteriores, na medida em que as respostas que os países deram a eles podem ter influído nas decisões acerca da magnitude e meio do ataque, além das considerações tradicionais de política externa dos países envolvidos. O fenômeno dissuasório presente em um caso não se dá em um vácuo, pois em se tratando de um fenômeno novo, qualquer indicação anterior pode e deve ser utilizada para sua compreensão. Além disso, casos posteriores podem apontar elementos construídos a partir das experiências anteriores, e em se tratando de episódios emblemáticos, a linha de influência, em geral, pode ser traçada.

Alguns analistas colocam na mesma categoria qualquer ataque cibernético que transcenda barreira nacionais[47]. (GAMERRO-GARRIDO,2014, BRANTLY,2014) A análise a ser conduzida aqui não se beneficia de uma categorização tão ampla; sendo assim, serão analisados apenas os casos com implicações de dissuasão entre países. Gamerro-Garrido

[47] O *think tank* CSIS – Center for Strategic and International Studies – atualiza constantemente uma lista com os principais incidentes cibernéticos desde 2006. Esses incidentes são definidos como ataques a agências governamentais, empresas do setor de defesa e empresas de alta tecnologia ou crimes econômicos com perdas de mais de um milhão de dólares americanos. Em julho de 2020 a lista possuía 48 páginas, com centenas de casos documentados. Dentro desses, poucos incidentes apontam diretamente para questões de dissuasão entre países. (A lista está disponível em <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>)

(2014) identifica 17 casos até 2013, enquanto Brantly (2014) identifica 7 casos mais impactantes até 2012.

Em se tratando de casos mais recentes, os ataques contra a Ucrânia em 2015, 2016 e 2017 podem ter seus aspectos de dissuasão analisados, pois as evidências são claras para utilização de armas digitais em ações conjuntas de guerra com elementos dissuasórios, principalmente sob as lentes da dissuasão cumulativa. Argumentar-se-á também que o caso das tentativas da Rússia de interferir em eleições de países ocidentais também se enquadra nessa moldura de análise, como operações de subversão.

Um aspecto percebido ao longo desta análise foi o aumento da presença da Rússia nas operações cibernéticas perpetradas contra outros Estados. Greenberg (2019) argumenta que a unidade russa conhecida como Sandworm é responsável por várias operações cibernéticas russas contra seus oponentes, com planejamento e operação coordenadas.

Em adição, estudos recentes demonstraram que as operações chinesas no ciberespaço foram constantes em grande parte dos períodos analisados. (LINDSAY; CHEUNG (2015); BRANTLY; VAN PUYVELDE (2019); FIREEYE (2019)) As operações chinesas aparentam estar em um contínuo e com alvos diversos ao longo dos anos; portanto, os casos específicos da atuação chinesa são mais difíceis de serem delimitados, ao contrário da maioria dos outros casos. Os grupos chineses que perpetram ataques também estão dentro de um contínuo entre grupos autônomos e grupos dentro do governo, passando por grupos patrocinados esporadicamente e grupos com aceitação governamental tácita de suas atividades.

Ao final do capítulo é feito um balanço dos debates sobre a evolução da dissuasão por meio dos casos analisados e se apresenta um quadro comparativo entre os casos estudados, com a categorização de tipos, atores participantes, principais ferramentas e respostas aos eventos.

2.1.OS PRIMÓRDIOS

Os primeiros casos de ataques cibernéticos entre Estados incialmente foram objeto de grande especulação acerca de seu potencial destrutivo. Incialmente, os únicos pontos de comparação acerca das possibilidades eram trabalhos de ficção científica ou da literatura cyberpunk.

Em 1993, a Rand Corporation publicou artigo intitulado "Cyberwar is coming!"[48] (ARQUILLA; RONFELDT, 1993) no qual foram propostos dois tipos de conflito: guerra cibernética (*cyberwar*) e guerra das redes[49] (*netwar*). A guerra cibernética seria focada em ações de comunicação e inteligência particularmente direcionadas contra infraestruturas de comando e controle. *A*s guerras de redes por sua vez, seriam operações de baixa intensidade com elementos da sociedade civil e outros atores não estatais, e exemplificada pela influência *online* de terroristas ou criminosos.

As primeiras acepções de guerra cibernética seriam então ações conjuntas e orquestradas em múltiplos domínios. Os exemplos que Arquilla e Ronfeldt fornecem correspondem a ações cibernéticas que objetivam reduzir a capacidade de coordenação, comando e controle de um inimigo, com subsequentes ataques cinéticos para tirar proveito dos impactos causados pelas reduções de opções de comunicação.

Os primeiros dois casos a serem analisados, Solar Sunrise e Moonlight Maze, foram interpretados, a seu tempo, a partir das ideias iniciais sobre guerra cibernética. Entretanto, ao contrário dessas ideias, eles não se deram sob nenhum contexto de guerra convencional.

Neste primeiro período, as capacidades de ataques cibernéticos não haviam se desenvolvido o suficiente para confirmar o impacto inicial previsto pelos primeiros analistas. Os impactos aquém do esperado contribuíram para a perda de importância das operações de guerra cibernética no imaginário militar. Um "*Pearl Harbor* cibernético" nunca ocorreu[50] e os eventos posteriores mostraram que o fenômeno se revelou muito mais como continuum do que como ruptura.

2.1.1. Solar Sunrise

O primeiro caso a ser analisado, retrospectivamente, não é um caso de dissuasão entre países. O ataque foi perpetrado por atores privados, com motivações particulares e, estaria, inicialmente, fora do escopo da presente análise. Entretanto, a forma peculiar como o defensor

[48] Publicado originalmente em Comparative Strategy, Vol. 12, No. 2, 1993. É interessante notar que ele é republicado em 1997, o que pode indicar uma influência relativamente longa nesse período inicial. (ver também: Arquilla, John e David Ronfeldt (1997)).
[49] Em traduções livres.
[50] Lawson e Middleton (2018) analisam como a ideia de "*cyber Pearl Harbor"* evoluiu entre 1991 até 2016 nos EUA e chegam a conclusão que a espera por esse momento de ruptura para investimentos maiores em defesa foi contraproducente em relação às operações cibernéticas conduzidas pela Rússia, que se aproveitou desse espaço de manobra de operações com impactos abaixo do nível físico. Ou seja, a espera dos EUA por ações disruptivas de sabotagem abriu espaço para ações contínuas de espionagem e subversão por parte da Rússia. Essa discussão será retomada no último capítulo desta tese.

(os EUA) lidou com o caso representou um interessante como "teste" sobre a maneira como as potencias poderiam agir frente a ações no domínio cibernético.

O ataque se deu em fevereiro de 1998, com a invasão de mais de 200 sistemas do Departamento de Defesa dos EUA (Nasa, Pentágono, Força aérea, entre outros). Os sistemas invadidos não eram classificados; entretanto, diversos sistemas de suporte importantes foram também atacados. Inicialmente a suspeita foi de que se trataria de um caso de espionagem iraquiana. Entretanto, após investigação envolvendo as principais agências norte-americanas (FBI, NSA, CIA, Nasa e outras) foi detectado que se tratava de apenas três pessoas, dois adolescentes californianos e um mentor israelense. (HILDRETH, 2001)

Portanto, as lições que foram tomadas do caso expuseram as falhas iniciais da estratégia dos EUA para lidar com ameaças no domínio cibernético. Hildreth, em relatório para o Congresso estadunidense de 2001 intitulado "Cyberwarfare", resume da seguinte maneira:

> *"Lessons some have drawn, however, are that Solar Sunrise confirmed the findings of Eligible Receiver: U.S. information systems are vulnerable. Additionally, others indicate that various legal issues remain unresolved (e.g., statutory restrictions and competing investigative needs and privacy concerns that hinder searches), there are no effective indications and warnings system in place, intrusion detection systems are insufficient, and there is too much government bureaucracy that hinders an effective and timely response".* (HILDRETH, 2001, p. 5)

Aqui argumenta-se que, embora ao final não tenha sido um caso de conflito entre países, as implicações em termos de capacidade dissuasória e, uma certa "postura dissuasória", podem ser encontradas no caso.

O caso se deu em meio a tensões geopolíticas devido à presença de inspetores de armamentos das Nações Unidas no Iraque. Inicialmente os ataques foram rastreados como tendo origem em algum lugar do Golfo Pérsico, por isso os investigadores inicialmente suspeitaram da participação do Iraque (KAPLAN, 2017).

Nesse caso, como em outros, os agressores utilizaram técnicas simples de roteamento para dar a impressão de que os ataques partiam de lugares diferentes. A partir do endereço IP de uma conexão é possível identificar, com certa precisão, o local de onde surgiu. Entretanto, é possível mascarar essa origem com determinadas técnicas. Ainda assim, a partir de uma

análise detalhada e do acesso a registros de operadoras de internet, é possível identificar a origem dos ataques[51].

Esse incidente demonstrou a importância do problema da atribuição. A investigação se baseou em uma suspeita de participação iraquiana logo no início, e os órgãos de inteligência dos EUA levaram essa suspeita ao Presidente norte-americano. Levando em conta as análises iniciais acerca de ações de guerra cibernética (ARQUILLA; RONFELDT,1993), um ataque desse tipo poderia ser prenuncio de um ataque cinético em conjunto. Entretanto, além da retórica, não foram fornecidas respostas imediatas. Naquele momento, as relações entre os EUA e o Iraque eram tensas e sérias consequências poderiam advir de uma atribuição errada. Um ataque cinético justificado por um ataque cibernético teria sido o primeiro exemplo do recurso a tal justificativa. Esse incidente revelou a importância da cautela para casos semelhantes seguintes, além de ter posto em relevo também o poder de ações diversionistas que um terceiro ator poderia ter ao manipular a atribuição de ataques.

Além disso, o incidente demonstrou a vulnerabilidade que acometia os sistemas de defesa dos EUA. O ataque evidenciou o baixo nível de proteção de diversos sistemas importantes de suporte diante de ataques cibernéticos; deixou patente, ademais, que um agressor mais sofisticado poderia ter causado grandes danos àqueles sistemas. Reforçou também o argumento da dominância do ataque[52] no âmbito cibernético, em contraposição à situação de dominância da defesa que eram frequentemente analisadas nos estudos de dissuasão na época da Guerra Fria[53].

As categorias de dissuasão discutidas anteriormente não são aplicáveis ao ataque em si. Porém, em se tratando de um cálculo de um possível agressor, a vulnerabilidade que

[51] Geralmente a impossibilidade de rastreio se dá quando algum operador no caminho de roteamento utilizado pelo agressor decide não cooperar com as investigações, ou quando legislações específicas dos países das operadoras de internet travam uma investigação, principalmente em se tratando de países sem acordos específicos em relação a isso. Com capacidade técnica suficiente e cautela um agressor individual pode ser anônimo. Entretanto, agressões estatais maiores, como demonstrado em diversos casos, são muito mais difíceis de serem escondidas totalmente, mesmo nos ataques mais elaborados. Ainda assim, a negação plausível não cessa, principalmente em se tratando de construção de cadeias de evidências longas e em jurisdições diversas.

[52] Brantly e Van Puyvelde (2019) argumentam pela dominância de ações ofensivas no meio cibernético, pois a quantidade de pontos de entradas em sistemas cibernéticos é muito maior do que a capacidade dos defensores em defender todos esses pontos. Posição contrária foi defendida por Morgan (2003) ao entender que os constantes desenvolvimentos tecnológicos gerariam uma situação de dominância da defesa por meio de capacidades defensivas cada vez mais sofisticadas tecnologicamente, como, por exemplo, o desenvolvimento do escudo antimísseis, que depende de tecnologia avançada para seu funcionamento.

[53] A situação de dominação da defesa gera estabilidade, pois um possível atacante teria que utilizar mais recursos para passar pelas defesas do que o defensor utilizou para organizá-las em primeiro lugar. A dominação do ataque faz com que o defensor tenha que utilizar mais recursos, o que leva a um cálculo favorável ao possível atacante e a menos estabilidade, com aumento do número de conflitos. Em se tratando de armas com menor potencial destrutivo do que armas atômicas, a situação de dominância do ataque poderia gerar várias ações abaixo dos limiares de resposta com armas nucleares.

acometia os sistemas dos EUA poderia ter tido o efeito de reduzir os possíveis custos previstos de um ataque, além de potencializar sua magnitude. As falhas iniciais de atribuição também seriam indicativas de que redirecionar a culpa para um terceiro, ao menos inicialmente, seria uma possibilidade para um agressor. Visto dessa maneira, o incidente, em sua totalidade, poderia ter implicado uma redução temporária da capacidade dissuasória dos EUA, ainda que envolvendo apenas atores não estatais.

Nenhum grande ataque aos EUA ocorreu imediatamente após o Solar Sunrise, ou foi atribuído, em sua origem, às vulnerabilidades reveladas no incidente. Portanto, qualquer eventual redução de capacidade dissuasória não foi suficiente para se atravessar o limiar de um ataque. Outros fatores podem ter contribuído para tanto, como a incapacidade técnica de algum possível agressor em tirar proveito de tal redução. Em 1998 as capacidades dos países de conduzir operações de guerra no ciberespaço eram certamente mais limitadas, e para tirar proveito de falhas dissuasórias um país deveria deter capacidades técnicas já consolidadas, além da vontade política de empreender um ataque dessa categoria.

Em uma leitura inicial, o caso apontaria a uma certa impossibilidade de dissuasão, em se tratando de ataques perpetrados por indivíduos. Entretanto, no que tange às relações entre países, o caso demonstrou a possibilidade do ataque e a facilidade de efetivá-lo. E, a despeito dessa possibilidade e facilidade, nenhum ataque desse tipo e com patrocínio de Estados aconteceu nos anos seguintes àquele evento. A vulnerabilidade dos sistemas de defesa cibernética dos EUA que ficou evidenciada então não foi suficiente para incentivar potenciais inimigos a perpetrarem ataques similares naquele período. Porém, não se pode descartar a possibilidade de que tais inimigos confrontem barreiras técnicas eles próprios. Embora, os ataques ocorridos no Solar Sunrise tenham sido relativamente simples, os mesmos demandaram certo nível de capacitação técnica talvez não facilmente acessível a atores eventualmente dispostos a perpetrá-los.

Para efeitos de cálculo dissuasório, a explicitação de uma fraqueza pode reduzir os custos ou aumentar os danos de um potencial ataque. A demonstração da fraqueza dos sistemas dos EUA nesse episódio ainda assim não estimulou um ataque; portanto, nenhum ator que estivesse apto a perpetrá-lo considerou que essa fraqueza era suficiente para ultrapassar o limiar da capacidade dissuasória em questão.

2.1.2. Moonlight Maze

As operações intituladas Moonlight Maze foram consideradas um dos primeiros casos de espionagem cibernética patrocinados, de fato, por um Estado (HAIZLER, 2017). As primeiras investigações sobre incursões russas nos sistemas dos EUA vieram a público em 1999, com a descoberta de ações cibernéticas de espionagem que teriam começado em 1996 e continuado até pelo menos 1998 (GUERRERO-SAADE *et al*, 2017). Também pode ser considerado como o primeiro caso de APT (*Advanced Persistent Threat*)[54].

Haizler (2017) resume a importância do caso:

> *"Mooonlight Maze was an important progression in cyber warfare and cybersecurity due to its implications on future conflicts. It pointed out the future shift in the modern battlefield from a kinetic war – in which enemies have names and physical locations, and in which attacks can be witnessed and assessed – into asymmetrical warfare with offensive cyber operations, where attacks might be invisible, adversaries are unknown, and damage is hard to quantify. The incident led to dramatic shifts in the US administration`s approach to cybersecurity*." (HAIZLER, 2017, pag. 34)

Os alvos das operações incluíam instalações militares, centros de pesquisa e universidades. Além dos EUA, outros países foram alvos, incluindo Reino Unido, Canadá, Alemanha e Brasil[55]. Os ataques não utilizaram ferramentas muito sofisticadas, mas se beneficiaram de diversas vulnerabilidades nos sistemas invadidos à época, as quais eram de conhecimento público. Até então, a segurança dos softwares não era considerada tão urgente pelas empresas desenvolvedoras; vulnerabilidades poderiam persistir por muitos meses mesmo após terem sido reveladas publicamente.

Durante a investigação, os EUA enviaram equipes à Rússia, esperando cooperação para elucidação do caso. Os investigadores chegaram a receber confirmação verbal de que o ataque havia sido conduzido por agências de inteligência da Rússia. Porém, a investigação

---

[54] Ameaças Avançadas Persistentes são situações em que atores mantém acesso não autorizado a sistemas de computador por longos períodos de tempo, por vezes meses ou até anos. Frequentemente são patrocinadas por Estados, pois a coleta de informações em longos períodos raramente beneficia atores que invadem sistemas em busca de ganhos econômicos imediatos. O termo "Avançado" se refere a sofisticação das ferramentas utilizadas por esses atores. (KASPERSKY, **What is and Advanced Persistent Threat (APT)?**, disponível em <https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats> acesso em 22.ago.2020.

[55] O analisa de cibersegurança Chris Doman analisou o caso a partir de documentos declassificados pelo governo estadunidense a partir de pedidos da lei de acesso à informação (FOIA- *Freedom of Information Act*). (**The First Cyber Espionage Attacks: How Operation Moonlight Maze made history**. (Doman, 2016) Disponível em <https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7> Acesso em 1.nov.2021.)

não obteve apoio russo após isso. (GREENBERG, 2019 e KAPLAN, 2017) Evidências mais recentes sugerem que o grupo ligado ao ataque ainda estaria ativo vinte anos depois[56].

Uma das consequências do ataque foi o expressivo aumento do investimento em segurança cibernética nos EUA, com definições mais claras de políticas em operações de guerra assimétricas. A Diretiva Presidencial 63 (PDD 63) foi, em parte, resposta a esse caso. A mesma determinou a criação do *National Incident Protection Center* (NPIC) e da *Joint Task Force Computer Network Defense*, o primeiro com objetivo de proteger infraestruturas civis e governamentais e o segundo com objetivo de centralizar a defesa militar e respostas a ataques cibernéticos. (HAIZLER, 2017)

Após a descoberta, o ataque não foi retaliado ou respondido e a própria identificação dos autores não foi conclusiva. Em termos de dissuasão cumulativa, a falha em reagir à altura poderia representar uma oportunidade perdida de definição de regras de engajamento e ainda poderia ser um convite a ações iguais ou mais impactantes no futuro. As evidências de que o mesmo grupo estaria ativo duas décadas depois pode indicar uma linha de aprimoramento dos atacantes. Já a demora na descoberta dessas evidências demonstra a capacidade do grupo em permanecer encoberto por um longo período, o que poderia implicar a existência de algum tipo de apoio ou patrocínio estatal.

2.2.DESENVOLVIMENTO E EMPREGO COORDENADO

Após esse período experimental de emprego de operações cibernéticas até o início dos anos 2000, as possibilidades de integração e a sofisticação dos ataques aumentou consideravelmente. Nesse período verificou-se o surgimento e a manutenção de grupos de atacantes cibernéticos coordenados e com acesso a amplos recursos. As unidades chinesas e russas de ataques cibernéticos ganharam primazia e passaram a ser as perpetradoras dos principais ataques até a descoberta do Stuxnet em 2010. Diversos grupos ativos na década de 2010-2020 começaram suas operações nessa década.

As operações de espionagem industrial e militar daquele período roubaram grande quantidade de informações por muitos anos, embora seja ainda difícil estimar, com qualquer margem de precisão, o impacto da utilização dessas informações.

---

[56] VICE. **New Evidence Links a 20-Year-Old Hack on the US Government to a Modern Attack Group.** Disponível em <https://www.vice.com/en_us/article/vvk83b/moonlight-maze-turla-link> acesso em 17.set.2020.

2.2.1. Espionagem industrial e vigilância chinesa: Operação *Titan Rain* e outras

Em 2005 foi revelado que a unidade chinesa de operações cibernéticas persistentes (Unidade 61398) estaria roubando segredos industriais dos EUA em larga escala e de maneira sistemática desde 2003[57]. Esses ataques foram nomeados como *Operation Titan Rain*. Lindsay e Cheung (2015) classificam esse caso como a primeira indicação pública de APT (*Advanced Persistent Threat*)[58] patrocinado por um Estado.

Hagestad (2012) classifica o caso *Titan Rain* como o primeiro de uma série contínua de ataques patrocinados pelo governo chinês, tendo como um dos objetivos principais o desenvolvimento de capacidades amplas de condução de operações de guerra cibernética. Segundo Hagestad, esses desenvolvimentos incluíram, posteriormente, capacidades de incursão em sistemas de distribuição e produção de energia elétrica nos EUA.

Após as primeiras descobertas, diversas outras operações de espionagem pela China nos EUA foram reveladas. Lindsay e Cheung identificam 37 casos de APTs patrocinados pela China até 2013. Segundo o relatório feito naquele mesmo ano pela Mandiant, a Unidade 61398 estaria ativa globalmente desde pelo menos 2006, com invasões identificadas a sistemas de 141 organizações, a maioria dos EUA.

Em 2011, o Escritório de Contra-Inteligência dos EUA (Office of the National Counterintelligence Executive) publicou relatório encaminhado ao Congresso intitulado "Foreign Spies Stealing US Economic Secrets in Cyberspace", com foco nas ações da China e da Rússia. Nesse relatório a China já era apontada como a perpetradora mais ativa e mais persistente de espionagem econômica.[59]

Brantly e Van Puyvelde (2019) analisam brevemente como esses casos resultaram ações dissuasórias por parte dos EUA contra a China, culminando na redução significativa das

---

[57] A primeira publicação acerca do ocorrido foi feita pela revista Time em setembro de 2005, disponível em <http://content.time.com/time/magazine/article/0,9171,1098961,00.html> Acesso em 04.Ago.2020. Nessa primeira publicação o foco foi na atuação do *whistleblower* responsável por revelar as informações, investigações muito posteriores é que identificaram a participação do governo chinês no caso. Essas investigações foram conduzidas pela empresa de segurança cibernética Mandiant (posteriormente adquirida pela FireEye) (BRANTLY; VAN PUYVELDE, 2019).

[58] Ver nota 42.

[59] OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE. **Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011**. 2011. Disponível em <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/616-oncix-foreign-spies-stealing-us-economic-secrets-in-cyberspace> Acesso em 19.set.2020.

ações de espionagem chinesa dez anos depois da primeira descoberta, em 2015[60]. Segundo esses autores, o recurso a variados modos de dissuasão, inicialmente diplomática e depois econômica, com ameaças de sanções, foi o fator fundamental para o seu sucesso. Entretanto, Lindsay e Cheung (2015) fornecem uma alternativa, ou suplementação, a esse argumento. Segundo esse argumento, o custo de utilizar quaisquer segredos industriais roubados seria alto, pois implica desenvolver capacidades específicas de como incorporar as tecnologias e ideias roubadas em um diferente ecossistema tecnológico. Além disso, Lindsay e Cheung argumentam que existiria um possível temor do próprio governo chinês de diminuição, no longo prazo, de capacidade de novos desenvolvimentos tecnológicos locais, diminuição esta advinda da troca de capacidades autônomas de pesquisa e desenvolvimento por capacidades de cópia.

Há evidências de que as atividades chinesas no espaço cibernético foram contínuas no tempo, sendo difícil sua classificação temporal e a análise de sua evolução nos moldes aqui propostos. Aparentemente, segundo os elementos apontados por Brantly e Van Puyvelde (2019), esse primeiro período (2003-2015) pode ser caracterizado de maneira separada do período mais recente (2016-2020). O primeiro período se caracteriza muito mais por ações de espionagem, militar e industrial, enquanto o segundo adiciona elementos de subversão às operações conduzidas.

2.2.2. Estônia 2007

Em maio de 2007 a Estônia foi alvo de uma série de ataques cibernéticos por cerca de três semanas. Os ataques eram do tipo DDOS (*Distributed Denial of Service*), em que um grande volume de pedidos de acesso a websites causa uma espécie de congestionamento, impedindo o tráfego normal de pacotes de informação. O ataque foi coordenado principalmente contra as infraestruturas cibernéticas do governo da Estônia e websites do sistema financeiro e de notícias.

O ataque foi atribuído a hackers russos, em retaliação à retirada de uma estátua nacionalista da época em que a Estônia era parte da União Soviética. Inicialmente a Estônia acusou diretamente o governo russo de patrocinar os ataques, sem, no entanto, apresentar

[60] A identificação da redução dos ataques após 2015 veio por meio da análise conduzida pela empresa de segurança norte-americana FireEye, anteriormente Mandiant.

evidências. As investigações levaram ao indiciamento de apenas um estoniano de origem étnica russa, mas as mesmas não tiveram apoio do governo russo.

Soesanto (2019) descreve a divisão entre os analistas da OTAN à época. Os analistas europeus consideraram o ataque como o início de uma era de ataques cibernéticos, com a demonstração das capacidades russas em operações de guerra híbrida. Por outro lado, os analistas estadunidenses consideraram que o ataque não era uma ameaça tão grande, já que os EUA sofriam diversos ataques similares há muitos anos sem grandes danos.

Além disso, Soesanto também aponta a diferença entre a comunidade técnica e os responsáveis por articular as políticas de segurança nacionais durante a condução do caso. Enquanto a comunidade técnica teve uma postura calma e controlada a comunidade política foi rápida em apontar culpados, sem as devidas investigações[61].

Segundo Libicki (2020), em comparação ao caso da Geórgia em 2008, esse ataque não foi seguido de um ataque cinético, nem foi parte de uma operação de guerra contra a Estônia, o que demonstra ter sido uma ação não coordenada com outros domínios. Um fator importante seria a capacidade dissuasória fornecida pelo pertencimento à OTAN. Um ataque aberto e óbvio seria alvo de retaliação da aliança; portanto, uma ação experimental e de difícil atribuição poderia garantir a realização de alguns objetivos estratégicos e sem tal retaliação.

A despeito da capacidade dissuasória propiciada pela OTAN, a Estônia considerou as operações como um ataque, e esperou, inicialmente, algum tipo de resposta conjunta do grupo. Greenberg (2019), aponta a inação da OTAN naquele momento. O artigo 5º. do Tratado da OTAN estabelece que um ataque a qualquer membro é considerado um ataque a todos, devendo ser objeto de respostas conjuntas. Porém, os outros membros não estavam dispostos a considerar estes incidentes como ataques. O artigo 4º. prevê consultas aos membros em casos de ameaças à segurança de um membro, mas mesmo a invocação deste artigo não foi permitida.

A inação da OTAN provavelmente foi fruto da negação plausível da autoria dos ataques, ou da baixa intensidade em termos militares (nenhuma vida estava em risco e nenhuma movimentação militar da Rússia foi identificada). Gelinas (2010) aponta que a Rússia aceitou tacitamente a atribuição dos ataques dois anos depois, por meio de declarações

[61] De maneira similar à condução do caso *Solar Sunrise.*

ambíguas de oficiais russos e admissão de apoio passivo a ações de "protesto" em resposta a "ações fascistas"[62].

Essa ação ainda poderia ter sido entendida como um teste russo dos limiares dissuasórios da OTAN. A inação em termos de respostas imediatas propiciou um ganho político à Rússia que deferiu um ataque a uma ação política-cultural da Estônia e saiu "ilesa". A retirada da estátua em Tallinn gerou alguns protestos das minorias étnicas russas na Estônia, principalmente na capital, mas o ataque cibernético gerou prejuízos para o país como um todo por cerca de um mês, o que é um tempo consideravelmente grande para a mobilização de recursos computacionais para o ataque e poderia demonstrar mais do que uma ação isolada de ativistas hackers (*hacktivists*).

A despeito da inação inicial da OTAN, as consequências e as respostas a esse ataque se manifestaram, mas em prazos maiores. Um ano após o ataque, a OTAN fundou em Tallinn o NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), com objetivo de avançar a pesquisa e o desenvolvimento em defesa cibernética, além de disseminação de lições aprendidas e boas práticas. O Centro foi responsável pela criação do Tallinn Manual[63], um guia sobre como leis internacionais já existentes se aplicariam no contexto de ataques cibernéticos e/ou guerra cibernética.

2.2.3. Geórgia 2008

Em contraste com o caso anterior, Libicki (2020) argumenta que o caso da Geórgia em 2008 é exemplo de que um conflito cibernético pode fazer parte de uma ação de guerra com ataques cinéticos. Os ataques começaram pouco antes da invasão da Geórgia pela Rússia, entre 8 e 12 de agosto de 2008, e se estenderam até algumas semanas depois. O efeito, segundo Libicki, pode ter sido o de evitar que a Geórgia expusesse sua versão dos eventos que estavam se desdobrando, além de complementar as ações de guerra tradicional então em curso.

A série de ataques consistiu principalmente em ações do tipo DDOS e similares, limitando o acesso aos sites da Geórgia pelo restante da Internet, além de interferências nas

[62] Gelinas (2019) deixa um aviso interessante para o futuro, contruído a partir das lições desse caso: "Future victims of cyber attacks, however, cannot rely on the attacker claiming victory as the default method of attribution." Embora, em alguns casos, seja correto assumir que parte do ganho estratégico de um país advenha da própria demonstração de capacidades, o que incentivaria um país a "declarar vitória".

[63] A versão revisada do Manual está disponível em: <https://ccdcoe.org/research/tallinn-manual/> acesso em 24.set.2020.

redes de telefonia móvel. Esse ataque pode ser classificado como primariamente como subversão, com um componente de sabotagem. Ele gerou vantagem do controle imediato da narrativa acerca dos fatos pela Rússia em detrimento da Geórgia. As ações de sabotagem de infraestrutura aparentemente foram sustentadas apenas por um curto período[64].

Esse controle das narrativas ocorreu apenas enquanto o ataque DDOS se dava, e não foi total, apenas parcial. As ações de sabotagem, principalmente em se tratando das interferências de redes de telefonia móvel, podem ter gerado vantagens militares, reduzindo os canais disponíveis de comunicação das forças militares da Geórgia. No geral, o caso parece ser um teste, em pequena escala, do potencial das operações no ciberespaço em conjunto com operações militares.

A maioria dos ataques conduzidos foram do tipo mais simples, mas capazes de efeitos de larga escala. Ataques do tipo DDOS não requerem muito planejamento ou muitos recursos e podem ser feitos com rapidez, caso necessário. Por outro lado, os efeitos podem ser mitigados rapidamente pelos alvos por meio de bloqueios e do aumento de capacidade da conexão de servidores. Ainda assim, quando se trata de ataques em conjunto, o tempo de resposta do defensor pode ser longo o suficiente para permitir um ataque cinético simultâneo, o que adiciona outro elemento disruptivo ao conflito em curso.

Em termos de atribuição do ataque, um DDOS pode ser ofuscado pela participação de um grande número de computadores de voluntários e redes de computadores comprometidos (*botnets*). No ataque à Geórgia, os organizadores apelaram para sentimentos nacionalistas e patrióticos de voluntários Russos, além de *botnets* já existentes controladas por agentes criminosos. Dessa maneira a atribuição não pode ser feita pelo endereço IP de cada computador atacante, mas sim com base nos indícios de quem estaria por trás da organização e coordenação das ações.

Greenberg (2019) aponta que alguns dos ataques cibernéticos na Geórgia parecem ter sido coordenados com a invasão Russa. Por exemplo, um ataque cibernético foi lançado contra sites de oficiais e de notícias da cidade de Gori momentos antes de um bombardeio

[64] O ataque teve várias facetas, segundo as informações apresentadas por Hagen (2012), seria possível indicar elementos de espionagem, com o redirecionamento de servidores da Geórgia para servidores Russos, potencialmente auxiliando em tempo real o ataque militar. Ações de subversão também poderiam ser identificadas na invasão de sites governamentais com vandalismo (*defacement*, no termo em inglês), com imagens de Hitler sendo comparadas ao líder georgiano. Hagen compara os efeitos desmoralizantes dessas ações a operações psicológicas (PSYOPS). Hagen ainda aponta o fato do ataque cibernético e invasão acontecerem ao mesmo tempo não ser uma mera coincidência, pois o emprego de tropas russas na Geórgia foi o primeiro uso fora de seu território em quase três décadas.

russo. Isso aponta para uma coordenação centralizada entre as ações cibernéticas e as ações de guerra cinética.

O ataque cibernético a Geórgia, ao final, não foi tão impactante. Ao contrário da Estônia, a Geórgia não era um país altamente conectado à Internet; portanto, os efeitos se fizeram sentir mais no controle da narrativa externa do que em interrupções de serviços essenciais.

O conflito havia começado pela expressa vontade do governo georgiano em ingressar na OTAN. A Rússia viu isso como uma afronta a seus interesses e à sua influência na região. A invasão como um todo pode ser entendida como uma operação visando a dissuadir a Geórgia de seguir nesse curso e, nesse sentido, foi completamente bem sucedida.

2.3.DESENVOLVIMENTOS RECENTES

Os ataques realizados nos últimos anos vão além dos DDOSs observados no período anterior, incorporando elementos mais sofisticados às ações, estas aparentemente bem planejadas e de longo prazo, com intrusões em sistemas durando por vezes por anos.

O caso do vírus Stuxnet marca o fim desse período intermediário de experimentação e o início do período de rápidos desenvolvimentos em termos de sofisticação dos ataques, principalmente em se tratando de ataques a sistemas de controle industrial e operações de subversão. O caso do Stuxnet é analisado em profundidade no próximo capítulo.

2.3.1. Ucrânia 2015, 2016 e 2017: Ataques às redes de energia elétrica e o vírus *NotPetya*

Em 23 de dezembro de 2015, a Ucrânia foi atingida pelo primeiro cyber ataque em larga escala a desativar parte da infraestrutura de eletricidade do país. Três empresas de distribuição de energia elétrica foram atacadas ao mesmo tempo, utilizando ferramentas já identificadas anteriormente pelos analistas de segurança, como o malware *BlackEnergy*, software malicioso capaz de atacar sistemas de controle industrial, como os utilizados pelas empresas de distribuição de energia. O ataque teria sido realizado pela unidade russa denominada Sandworm[65]. (GREENBERG, 2019)

[65] Este nome foi dado pelos analistas de segurança que identificaram o grupo por meio das referências deixadas pelos atacantes ao livro Duna de Frank Herbert.

O ataque começou na capital, Kiev. Em um curto espaço de tempo, 30 subestações foram desativadas, e o firmware responsável pelo controle de aparato crítico foi reescrito em 16 das subestações, impedindo a recuperação imediata.[66]

Um ano depois, em dezembro de 2016, a rede de energia elétrica da Ucrânia foi novamente atingida por ataques cibernéticos. Desta vez o ataque foi localizado em uma subestação de distribuição e durou apenas uma hora. Em paralelo o Ministério da Finanças foi atacado, tendo servidores e acesso a serviços online comprometidos por alguns dias. Um terceiro ataque foi feito contra o sistema estatal de transportes ferroviários, com uma intrusão e um DDoS concomitante[67]. Alguns analistas classificaram esse ataque mais como uma demonstração de capacidades, pois embora a sofisticação das ferramentas utilizadas tenha sido grande o escopo do ataque foi pequeno, tendo duração baixa e alcance limitado. (LITSCHKO, 2017)

Alguns meses depois, em meados de 2017, a Ucrânia foi atingida por mais um ataque cibernético, o vírus *NotPetya*. Este ataque foi, até então, um dos maiores já ocorridos em termos de danos econômicos: estima-se em 10 bilhões[68] de dólares o total de danos a empresas e governos ao redor do mundo. O vírus foi chamado de *NotPetya*, em função de sua similaridade com o *ransomware* ocorrido no ano anterior chamado Petya, porém adicionado o *Not*, pois a função de recuperação dos dados criptografados estava propositadamente desativada.

Ransomwares são programas maliciosos capazes de criptografar o conteúdo de discos rígidos de maneira a evitar o acesso aos dados pelo proprietário. A criptografia utilizada garante que, se implementada corretamente, a descoberta da chave de acesso seja matematicamente impossível dentro dos paradigmas atuais da computação[69]. A maioria dos *ransomwares* possuem uma maneira de destravar a criptografia dos dados. Em geral, a chave de acesso é fornecida pelo agente malicioso após um pagamento irrastreável realizado em criptomedas (como *bitcoin* ou *ethereum*).

---

[66] WIRED. **Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. 2016.** Disponível em < https://www.wired.com./2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> acesso em 09.maio.2021.

[67] VICE. **The Ukrainian Power Grid Was Hacked Again.** Janeiro 2017. Disponível em <https://www.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report>Acesso em 13.set.2020.

[68] WIRED**. The Untold Story of NotPetya, the Most Devastating Cyberattack in History**. Disponível em <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> Acesso em 13.set.2020

[69] Embora, no futuro, a computação quântica possa modificar isso.

No caso do ataque à Ucrânia, em 2017, o *ransomware* utilizado apenas criptografava os arquivos das máquinas infectadas sem fornecer alternativa de pagamento de resgate. Isso leva a crer que o objetivo foi apenas de causar danos, sem perspectivas de ganhos pelos agentes que implantaram o vírus.

A falta de cuidado adequado pelos perpetradores do ataque fez com que o vírus se espalhasse por diversas empresas ao redor do mundo, incluindo operadores de portos de carga e hospitais, com diversos sistemas informatizados comprometidos, necessitando reconstrução e reversão a operações manuais em alguns casos.

Em 2018, os EUA e o Reino Unido declararam que a Rússia teria implementado o ataque[70]. A declaração feita pelo Secretário de Imprensa da Casa Branca classificou o evento como o ataque cibernético mais destrutivo e mais custoso da história. Além disso, ameaçou consequências: "*This was also a reckless and indiscriminate cyber-attack that will be met with international consequences*"[71].

As consequências[72] vieram em março de 2018 na forma de sanções dos EUA a três entidades russas e treze indivíduos russos acusados de perpetrar ou auxiliar em ataques cibernéticos. O conjunto de sanções foi justificado como tendo mais de um fenômeno causador, incluindo as operações de subversão da Rússia na campanha eleitoral norte-americana de 2016.

Em termos de dissuasão cumulativa, a resposta não foi proporcional e nem rápida. A ausência destes fatores pode resultar em baixa capacidade dissuasória contra ações similares futuras (como argumentado por Tor (2015)), além de ser uma oportunidade não plenamente realizada de definir as regras futuras do jogo. A continuidade dos ataques à Ucrânia demonstra, em parte, a incapacidade dissuasória do país no período. Nenhum dos ataques foi respondido de maneira rápida; portanto, os atacantes puderam continuar as operações, entendendo que os ganhos políticos ou estratégicos poderiam ser mantidos após os ataques.

---

[70] WASHINGTON POST. **Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes.** Disponível em <https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html> acesso em 13.set.2020; THE REGISTER. **UK names Russia as source of NotPetya, USA follows suit**. Disponível em <https://www.theregister.com/2018/02/15/uk_names_russian_military_as_source_of_notpetya/> acesso em 11.out.2020.

[71] WHITE HOUSE. **Statement of the Press Secretariat**. Disponível em <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/> acesso em 27.jul.2020.

[72] US DEPARTMENT OF TREASURY. Press Release. **Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks** disponível em <https://home.treasury.gov/news/press-releases/sm0312> acesso em 24.set.2020.

Além disso, os ataques poderiam servir como teste de capacidades e de tempo de reação dos defensores, de modo a fornecer insumos para desenvolvimento de ataques futuros.

A inação em termos dissuasórios, ou a ação lenta e pouco proporcional, pode também gerar consequências em termos de desenvolvimento e de "estoque" de armas cibernéticas. Litschko (2017) argumenta que os vazamentos de informações de que os EUA estariam estocando vulnerabilidades em sistemas cibernéticos[73] poderiam gerar um sentimento de que a Rússia poderia também fazer o mesmo. Baixa atividade dissuasória (em termos de dissuasão cumulativa), aliada ao conhecimento do desenvolvimento de armas por nações rivais poderia até levar a uma corrida armamentista cibernética.

Uma corrida armamentista cibernética poderia se caracterizar por pequenos episódios de demonstração de capacidades, com ataques sofisticados, mas de baixa intensidade, como incursões em sistemas muito protegidos e vitais, mas com perturbações pequenas, como na Ucrânia em 2016. Um teste autônomo e isolado, nos mesmos moldes dos testes nucleares, teria menos poder demonstrativo de capacidades, pois seria difícil provar que o desenvolvedor da arma em questão não modificou ou alterou os sistemas defensores que fizeram parte do teste. Portanto, existiriam incentivos para a realização de operações "ao vivo", com alta sofisticação, mas de baixa intensidade.

Caso o ataque à Ucrânia em 2016 venha a se provar como um ataque de demonstração de capacidades, altera-se uma das premissas iniciais do desenvolvimento de armas cibernéticas. Nas concepções iniciais sobre o tema, um dos problemas encontrados é o da baixa duração de armas cibernéticas desenvolvidas, isto é, uma vez encontrado um ponto de ataque em um software espera-se que uma atualização vá corrigir a falha em um curto período de tempo. Assim, haveria incentivos para o emprego das armas cibernéticas assim que desenvolvidas. Além disso, após qualquer ataque, as falhas dos softwares seriam rapidamente consertadas pelos defensores; portanto, uma ação de demonstração seria, a princípio, um desperdício de recursos. Porém, o outro lado do desenvolvimento de armas cibernéticas é o lado das capacidades humanas. Ações demonstrativas usariam recursos e armas desenvolvidas, mas não seriam tão custosas, pois mesmo o país alvo tendo desenvolvido novas defesas cibernéticas, o desenvolvimento de capacidades técnicas, em termos de capital

[73] Litschko se refere aos vazamentos de documentos confidenciais da CIA, contendo, entre outras, informações, desenvolvimentos de armas cibernéticas, incluindo uma grande quantidade de ferramentas desenvolvidas. Esse vazamento foi chamado de "Vault 7" e foi disponibilizado pelo Wikileaks em março de 2017. (WIKILEAKS. **Vault 7: CIA Hacking Tools Revealed.** Disponível em <https://wikileaks.org/ciav7p1/> Acesso em 13.set.2020)

humano, do país atacante se manteria e talvez até seja melhorado no curso desse tipo de "exercício".

2.3.2. Ações chinesas contínuas de espionagem industrial e subversão

Em 2018, o escritório de contra inteligência dos EUA, segundo a mesma lógica do Relatório apresentado em 2011, publicou novo relatório sobre a espionagem econômica no ciberespaço. Novamente o foco recaía sobre a China e a Rússia[74]. Entretanto, neste relatório é citada a diminuição das atividades maliciosas chinesas no espaço cibernético após os compromissos entre os EUA e a China de 2015, como apontado por Brantly e Van Puyvelde (2019).

Análises mais recentes da empresa de segurança FireEye identificaram novos focos de atividade de APT chineses, principalmente nos meses anteriores à redação desta tese. A FireEye denomina o grupo de realizadores dessas atividades como "APT41". No relatório de 2018 do escritório de contra inteligência dos EUA este APT ainda não havia sido mencionado, embora seja possível que algumas das ações mencionadas fossem atribuídas posteriormente a esse grupo.

Esse aumento de atividade pode apontar para uma redução da capacidade dissuasória dos EUA recente; segundo o paradigma de dissuasão cumulativa, a retaliação deveria ser feita de maneira a determinar as regras de engajamento, de maneira rápida e inequívoca. Algumas medidas de sanção econômica estão em curso, como o bloqueio de aplicativos chineses de redes sociais e comunicação e da participação da China na implantação das redes de telefonia 5G, mas o quanto isso está sendo comunicado como ações de retaliação contra atividades de espionagem ainda é apenas objeto de especulação. Parte das ações é justificada como proteção de indivíduos norte-americanos contra a espionagem em massa chinesa. Contudo, em comunicações públicas ainda não associam tais ações à retaliação por ações passadas.

No relatório produzido pela FireEye em 2019, a unidade APT41 é classificada como de utilização dupla, para espionagem patrocinada pelo Estado e para cyber crimes financeiros,

[74] Com um novo ator desta vez, o Irã, classificado como uma ameaça em ascensão, mas com capacidades similares as da China e Rússia. Segundo a primeira página do relatório: "China, Russia, and Iran stand out as three of the most capable and active cyber actors tied to economic espionage and the potential theft of U.S. trade secrets and proprietary information." (OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE. **Foreign Economic Espionage in Cyberspace.** 2018. Disponível em <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf> acesso em 19.set.2020.)

potencialmente para ganho próprio. A análise aponta para a atuação dessa unidade em pelo menos 14 países desde 2012, mas com foco em empresas de alta tecnologia nos EUA. Ações subversivas também foram identificadas, como a coleta de informações, vigilância e tentativa de influência nos protestos democráticos em Hong Kong.

A diminuição nas operações cibernéticas maliciosas da China após 2015 aponta para um certo nível de coordenação entre os diversos grupos de APTs chineses. A FireEye identifica onze grupos, com variados graus da possível ligação com o governo chinês, desde grupos praticamente autônomos a grupos possivelmente operados pelas próprias forças armadas. O aumento recente das operações pode ser, em parte, coordenado e, em parte, oportunístico, pelos grupos autônomos. Com a existência de grupos não governamentais, as ações de dissuasão que os EUA poderiam empreender teriam sua efetividade reduzida, pois grupos que operam visando ganhos econômicos só poderiam ser propriamente impedidos de operar caso o governo chinês estabelecesse incentivos negativos dentro de sua jurisdição. Ainda assim, as operações mais impactantes aparentemente têm origem em grupos ligados ao governo, o que torna a dissuasão a nível interestatal possível.

2.3.3. Influência russa nas eleições americanas e britânicas

Em termos de dissuasão militar, a comparação de ações de subversão em procedimentos de regimes democráticos com operações tradicionais de guerra pode parecer incorreta. Entretanto, as ações de subversão, nesse caso, podem ser alvos de procedimentos dissuasórios, tanto econômicos como diplomáticos ou, até mesmo, militares. A categorização desses eventos pelos seus alvos frequentemente os compara a ataques cibernéticos. Analistas, como Jamieson (2018), argumentam que o caso da interferência russa nas eleições de 2016 deve ser entendido como um caso de guerra cibernética a despeito de seu impacto não ser comparável a um ataque cinético.

Em 2016, na eleição presidencial dos EUA, diversos pontos de interferência russa foram identificados. As ações se caracterizaram por uma campanha contínua de dispersão de informações falsas ou distorcidas, utilizando, como principal plataforma, as redes sociais (Twitter, Facebook, Reddit e outras). A campanha de dispersão de informações falsas provavelmente começou alguns anos antes, em 2014 ou 2013, mas teve um aumento considerável em 2015 após a nomeação dos candidatos dos partidos. Outro ponto de ataque foram invasões a contas de e-mails ligadas aos profissionais da campanha de Hillary Clinton.

Diversas informações foram roubadas e compartilhadas com o site Wikileaks, que publicou uma série de informações negativas pouco tempo antes das eleições, distraindo o eleitorado norte-americano e potencialmente alterando o resultado das eleições[75].

A análise da Rand Corporation (POSARD *et al*, 2020) identificou como as estratégias de influência russa foram adaptadas de maneira muito precisa a cada público-alvo. Eleitores da extrema direita receberam conteúdos conspiracionistas, facilmente compartilháveis, enquanto eleitores afro-americanos receberam conteúdos sobre supressão de votos, com vistas a reduzir a participação eleitoral deste grupo. Eleitores religiosos receberam mensagens contra relações homoafetivas e assim por diante, com cada grupo recebendo mensagens confeccionadas com o objetivo de maximizar o impacto e a chance de aceitação e internalização. A criação destes conteúdos era feita tanto por pessoas reais (*trolls*[76]) quanto por robôs automatizados (*bots*[77]). Outra frente de ataque foi a criação de uma grande quantidade de narrativas díspares e conflitantes, com vistas a gerar confusão e descrença generalizadas nos sistemas eleitorais, gerando uma subsequente apatia do eleitorado.

Jamieson (2018) aponta os relatórios das três principais agências de inteligência dos EUA (FBI, CIA e NSA) e as declarações e votos dos Congressistas, que tiveram acesso a materiais classificados, como evidência que os EUA possuíam provas suficientes da interferência russa nas eleições[78].

A identificação das ações ocorreu durante o processo eleitoral, embora a atribuição ainda não pudesse ser confirmada com certeza. Jamieson (2018) e Isikoff e Corn (2018) apontam que a administração Obama chegou a considerar uma resposta com ações de ataques cibernéticos direcionados contra a Rússia, mas que possivelmente isto não ocorreu por medo de escalada de conflitos.

As primeiras respostas vieram tempos depois, em 2017, com as sanções a alguns indivíduos russos envolvidos nos ataques e que foram identificados. Os Congressistas dos

[75] Time Magazine. **Here's What We Know So Far About Russia's 2016 Meddling**. Abril 2019. Disponível em <https://time.com/5565991/russia-influence-2016-election/> Acesso em 27.set.20

[76] O termo *troll* é frequentemente utilizado para se referir a indivíduos que geram propositadamente discórdia, buscando respostas emotivas, com alto poder de engajamento na rede e subsequente compartilhamento e dispersão das mensagens desejadas.

[77] *Bots* aqui se refere a programas automáticos capazes de interagir com usuários (robôs). A utilização de *bots* em aplicações web é antiga, a própria criação de conteúdos automáticos por esse meio não é recente, entretanto, nos últimos anos, com o refinamento dos algoritmos e a popularização de tecnologias de aprendizado de máquina a capacidade de convencimento destas ferramentas aumentou muito.

[78] Além disso, para a construção de elementos de prova da interferência, diversas outras técnicas foram utilizadas, como a análise de conteúdo e metadados de postagens em redes sociais, o rastreio dos endereços de IP, a análise de semelhanças semânticas entre diferentes perfis utilizados por um mesmo operador ou grupo de operadores, entre outras.

EUA foram quase unânimes na votação que puniu tais indivíduos[79]. Outras sanções foram implementadas nos anos subsequentes, com foco em indivíduos[80]. O efeito dissuasório que as respostas tiveram possivelmente poderá ser analisado alguns anos após as eleições presidenciais de 2020, utilizando técnicas similares de análise em relação a 2016[81]. O efeito dissuasório pode ter se dado em outras esferas de ataques cibernéticos, mas a comparação com as eleições de 2020 aparenta ser um caminho analítico simples e direto para julgar o efeito que as respostas causaram.

2.4.BALANÇO DA DISSUASÃO NAS OPERAÇÕES CIBERNÉTICAS ANALISADAS

A natureza e a intensidade dos ataques cibernéticos parecem guardar relação com a capacidade de resposta dos atores envolvidos. Os ataques feitos pela Rússia nos países de sua antiga esfera de influência foram aumentando de intensidade no período analisado, adicionando elementos de sabotagem a ações de subversão e potencialmente espionagem. Enquanto isso, as ações de Rússia e China contra os EUA e outros países ocidentais não incluem ações de sabotagem, apenas a espionagem e a subversão. Desse modo, estar-se-ia, possivelmente, frente à capacidade dissuasória dos EUA (e talvez membros da OTAN) suficiente para limitar as ações de sabotagem, mas não suficiente para limitar as outras ações.

A expectativa inicial de que um evento com consequências físicas drásticas, como um Pearl Harbor cibernético, iria alterar profundamente o pensamento de defesa dos Estados Unidos não ocorreu, e inclusive pode ter sido catalisadora das operações de menor intensidade até agora (LAWSON; MIDDLETON, 2019). Entretanto, a presença de operações de influência nas eleições de países ocidentais pode ter impactos de alta intensidade, já que a instalação de governos mais amigáveis ao adversário em questão pode ser uma fonte importante de ganhos estratégicos e políticos. A espera de uma ação de alto impacto em infraestruturas (em ações de sabotagem) para a reorganização de um pensamento de defesa cibernética, principalmente nos EUA, em conjunto com o medo de escalada e com a

[79] O ato aprovado pelo Congresso dos EUA foi o Countering America's Adversaries through Sanctions Act (CAATSA), que também colocou sanções ao Irã e Coréia do Norte.

[80]UNITED STATES OF AMERICA. **United States Sanctions Russian Actors and Proxies for Efforts to Interfere in Elections.** Disponível em <https://www.state.gov/united-states-sanctions-russian-actors-and-proxies-for-efforts-to-interfere-in-elections/> Acesso em 10.Out.2020.

[81] Técnicas novas podem ser utilizadas pelos atacantes, assim como pelos investigadores. De qualquer modo, a prevalência deste tópico como assunto de mídia possivelmente gerou um efeito defensivo no eleitorado dos EUA, tornando-o mais resistente a interferências no ciclo eleitoral mais recente.

incapacidade de atribuição rápida de ataques, pode ser a causa da existência de um ambiente propenso a ações cibernéticas de alto impacto subversivo, mas sem elementos de sabotagem.

No caso da Ucrânia, onde foram identificadas ações de sabotagem, estas ocorreram dentro de um conjunto de outras ações militares, o que talvez explique o seu uso no caso. Um país que já estivesse disposto a invadir militarmente outro poderia obter ganhos adicionais ao utilizar elementos de ataques cibernéticos. A dependência de praticamente todos os países na infraestrutura de acesso a redes de computadores fez com que a utilização de ações cibernéticas em contextos militares deixe de ser apenas um experimento e passe a ser parte do arsenal de guerra.

Para além de uma nova arma em um arsenal, a adição de armas cibernéticas é uma evolução da ideia de operações em domínios múltiplos. Em publicação de 2017[82], o Exército dos EUA conceitua a ideia de operações em múltiplos domínios como possíveis respostas aos desafios à dissuasão em operações inimigas em subversão, operações de guerra informacional e operações de guerra não convencionais (nos termos em inglês: *subversion, information warfare(IW), unconventional warfare(UW)*). É interessante notar que os aspectos de sabotagem cibernética física não são muito discutidos no texto, implicitamente igualando os impactos e potenciais respostas a ações convencionais de guerra.

Em se tratando de dissuasão cumulativa, a capacidade de cada país demonstra grande variabilidade. Os países menores que foram alvos da Rússia provavelmente têm pouca capacidade de influir negativamente sobre as operações que a Rússia estaria disposta a conduzir após os ataques em outros países. Inclusive, o sucesso que a Rússia obteve no caso da Geórgia, ao impedir a sua filiação à OTAN, e o sucesso em atacar a Estônia sem sofrer consequências imediatas, podem ter sido catalisadores para as ações contra a Ucrânia anos depois, pois as operações se demonstraram mais impactantes e mais ousadas. E ainda assim, a resposta dos países da OTAN foi pequena e tímida, feita muito tempo depois dos ataques e sem consequências graves para a Rússia.

Em resumo, a incapacidade de resposta à altura a ataques descobertos é uma constante nos períodos analisados. As respostas, quando existentes, se dão meses ou anos após os ataques, quando o atacante já havia colhido os benefícios dos ataques. Essa demora geralmente se dá por dificuldades de atribuição e por medo de escalada de conflitos. Isso pode

[82] US ARMY. **Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040.** 2017. Disponível em <https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf> Acesso em 20.Set.2020.

ser um incentivo para uma maior sofisticação e amplitude dos ataques em ações futuras, revelando falha dissuasória em qualquer um dos paradigmas dissuasórios anteriormente demonstrados.

A dificuldade de atribuição é outro ponto que atacantes cibernéticos podem aprimorar, além da sofisticação técnica e da amplitude, tendo em conta as experiências aduzidas até agora. A relutância em retaliar de maneira errada gera uma grande janela temporal para a coleta de benefícios dos ataques. Ações diversionistas ou aumento da sofisticação das técnicas de ofuscação de ataques são elementos a serem analisados em casos futuros.

As ações recentes da China mostram que a espionagem industrial ainda é um fenômeno importante para a indústria chinesa, ainda mais em se tratando de tecnologias mais avançadas. A capacidade que os EUA demonstraram em diminuir a intensidade dessa espionagem em 2015 não se manteve e o aumento recente deixa patente uma diminuição do acumulado de capacidade dissuasória dos EUA. As ações recentes dos EUA contra algumas grandes empresas chinesas[83] podem ter impacto dissuasório, mas ainda não é possível ser conclusivo a esse respeito.

Embora ações de sabotagem sejam as mais visivelmente e imediatamente impactantes, como nos casos do Stuxnet e da Ucrânia, os impactos das ações de subversão e espionagem tendem a ter efeitos mais prolongados. Os ataques baseados em ações de subversão e espionagem tendem a durar mais e a gerarem respostas mais lentas. Ações de sabotagem podem ser demonstradas pelo defensor, mas ações de subversão podem minar exatamente a capacidade de controle da narrativa externa, tendo o efeito de, dentre outros, reduzir a velocidade ou o escopo de uma resposta internacional, como no caso da Geórgia.

A incapacidade de resposta a ações de subversão e espionagem decorre de diversas razões, mas a mais citada, nos casos estudados, foi a incapacidade de atribuição rápida e inequívoca dos ataques. Outra razão é o baixo impacto em termos de vidas em risco: quando vidas não estão imediatamente em risco há menos urgência em se tratando de respostas nos

[83] Restrição a operações da Huawei, fornecedora, dentre outros, de equipamentos para implementação de redes 5G, e às operações da empresa ByteDance, dona do aplicativo TikTok. Em 6 de Agosto de 2020 a Casa Branca publicou a *Executive Order on Addressing the Threat Posed by TikTok* (disponível em https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/ acesso em 15 de setembro de 2020) estabelecendo que o aplicativo seria uma ameaça à segurança dos EUA. Em 15 de Maio de 2019, a Casa Branca publicou a *Executive Order on Securing the Information and Communications Technology and Services Supply Chain* (disponível em https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ acesso em 15.set.2020) onde é claramente expresso a preocupação com a espionagem industrial e econômica contra os EUA. Essa ordem estabeleceu a restrição a compra de equipamentos 5G de "nações adversárias".

domínios militares. E mesmo em ações com elementos de sabotagem, respostas à altura não foram imediatas em nenhum caso. A expectativa é que, neste contexto, qualquer capacidade dissuasória seja diminuída, sugerindo uma situação de dominação do ataque, o que sugere uma condição instável e com constantes incentivos para os atores continuarem atacando.

Nesse contexto, os atores mais dispostos a atacar tentariam obter ganhos estratégicos ou políticos com ações abaixo dos limiares de resposta. E os próprios limiares de resposta tenderiam a ser testados continuamente, tanto em termos de intensidade dos ataques como em sofisticação das ferramentas (ou armas) utilizadas. A continuidade dos ataques à Ucrânia pode ser entendida desta maneira, com o primeiro ataque intenso, o segundo ataque sofisticado e com intenções de demonstração de capacidades e teste de limiares dissuasórios e o terceiro ataque ainda mais intenso e sofisticado com vistas a atingir grandes ganhos estratégicos.

Tabela 1: Resumo de classificação dos casos analisados

Caso	Ano	Tipo	Atores principais	Ferramentas utilizadas	Respostas
Solar Sunrise	1998	Não aplicável	EUA e atores privados	Exploração de vulnerabilidades	
Moonlight Maze	1996-1998	Espionagem	EUA e Rússia	Exploração de vulnerabilidades	Diretiva Presidencial 63
APTs Chineses	2003-contínuo	Espionagem e subversão	China e EUA	Diversas ferramentas	Sanções diplomáticas e ameaças de sanções econômicas
Cibertaque a Estônia	2007	Sabotagem	Estônia e Rússia	DDOS	Criação da CCD COE. Criação dos Manuais de Tallin.
Ciberataque a Geórgia	2008	Sabotagem e Subversão	Geórgia e Rússia	DDOS	
NotPetya e atques à Ucrânia	2015, 2016 e 2017	Sabotagem	Rússia, Ucrânia e outros	Ransomware e outras	Sanções dos EUA
Influência russa nas eleições dos EUA e RU	2016	Subversão	Rússia, EUA, RU	Desinformação em redes sociais e invasões a sistemas.	Sanções dos EUA

Fonte: elaborado pelo autor.

No próximo capítulo, será analisado o caso do Stuxnet, como o caso de sabotagem mais impactante em todos os períodos estudados. Será também demonstrado como os casos deste capítulo se relacionam àquele e quais conclusões acerca da dissuasão em guerra cibernética podem ser derivadas do conjunto dos casos analisados.

3. ANÁLISE DO CASO STUXNET

O vírus Stuxnet é frequentemente citado na literatura como o primeiro caso de emprego de uma arma cibernética com efeitos similares a um ataque convencional (FARWELL; ROHOZINSKI, 2011; ZETTER, 2015; HAMDOUNI, 2017). O mesmo será analisado de maneira separada neste capítulo, pois, por ser um dos casos mais bem documentados, proverá aportes analíticos fundamentais ao presente estudo. Para tanto, neste capítulo, apresentam-se, inicialmente, aspectos contextuais para, em seguida, proceder a análise do vírus em si; finalmente, delineia-se uma definição metodológica específica para o caso em estudo. Após isso, as hipóteses definidas na seção metodológica serão discutidas.

Esse caso consistiu de um vírus, provavelmente desenvolvido pelos EUA e Israel, utilizado para sabotar parte da capacidade de desenvolvimento de tecnologias nucleares do Irã. A principal parte do ataque se deu em 2009 e 2010[84], tendo como alvo as centrífugas da usina de enriquecimento de urânio do Irã na cidade de Natanz. Entretanto, o desenvolvimento do vírus é mais antigo, tendo início em torno de 2006, com a autorização de desenvolvimento por parte do Presidente norte-americano George Bush, ou, possivelmente, em 2003, com a interceptação, pelos EUA, de um cargueiro da Líbia contendo equipamentos de enriquecimento de urânio iguais aos utilizados pelo Irã.

O vírus é um caso emblemático, pois demonstrou de maneira inequívoca o potencial de destruição física que um vírus de computador pode infligir. Um ataque cinético como, por exemplo, o lançamento de um míssil, poderia ter tido efeitos similares em redução de capacidade de enriquecimento de urânio do Irã, mas teria tido consequências militares e diplomáticas muito diferentes, precipitando, muito provavelmente, uma guerra na região.

O caso se encaixa na categoria de sabotagem. Entretanto, é razoável supor que ações de espionagem foram utilizadas para o desenvolvimento e possível implantação do vírus nas usinas. Em 2019, alguns periódicos noticiaram que um possível agente holandês o teria implantado.[85] Em adição, o caso é interessante para a análise da dissuasão cumulativa, pois os

---

[84] Há evidências de que uma primeira versão do vírus teria sido utilizada em 2007, mas com efeitos muito mais sutis e menores investimentos técnicos. (LANGNER, 2020) Para este estudo será considerado o período do ataque mais impactante de 2009 e 2010.

[85] THE TIMES OF ISRAEL. **'Dutch mole' planted Stuxnet virus in Iran nuclear site on behalf of CIA, Mossad**. Disponível em <https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site-report/>, acesso em 09.Maio.2021. INFO SECURITY GROUP. **Dutch Insider Deployed Stuxnet: Report.** Disponível em <https://www.infosecurity-magazine.com/news/dutch-insider-deployed-stuxnet/> Acesso em 09.Maio.2021.

conflitos relacionados ao programa nuclear iraniano perpassam muitas décadas e os efeitos cumulativos das ações com fins dissuasórios dos outros países poderiam ser percebidos.

Em relação ao emprego do vírus e às escaladas das tensões relacionadas ao programa é interessante analisar o Irã pelo menos a partir de 2003, quando ocorreram as primeiras inspeções da Agência Internacional de Energia Atômica, tendo o país posteriormente concordado em assinar o Protocolo Adicional[86], permitindo um maior acesso dos inspetores às instalações nucleares. Ainda assim, ao se entender o histórico e o contexto é importante apontar que o desenvolvimento nuclear iraniano teve início cerca de quarenta anos antes, carregando, portanto, uma grande bagagem de tentativas, experimentos, conflitos políticos e conhecimentos científicos.

3.1.CONTEXTO

O histórico de desenvolvimento nuclear do Irã teve início com o desenvolvimento de tecnologias nucleares na década de 1950 no marco do programa norte-americano Atoms for Peace. A cooperação incluiu o repasse de conhecimentos por meio de treinamento de pesquisadores e a transferência de um reator de pesquisa para o Irã em 1967. A França também forneceu apoio, por meio de cooperações técnicas e investimentos conjuntos em reatores. Em 1979, com a revolução iraniana, essas parcerias se encerraram. Entretanto, as pesquisas nucleares iranianas prosseguiram, com apoios da China, Rússia e Paquistão.

A despeito da adesão do Irã ao Tratado de Não Proliferação Nuclear (NPT) em 1970 e da presença de inspetores da Agência Internacional de Energia Atômica (AIEA) no país, os EUA constantemente suspeitavam da existência de enriquecimento de urânio clandestino para o desenvolvimento de armas atômicas. Em 2003, a AIEA começou uma investigação cujos resultados foram publicados em 2011, com evidências de que, pelo menos até 2003 o Irã havia se engajado em atividades de pesquisa para desenvolvimento de armas nucleares.

[86] O Protocolo Adicional (a nomenclatura oficial do documento é “MODEL PROTOCOL ADDITIONAL TO THE AGREEMENT(S) BETWEEN STATE(S) AND THE INTERNATIONAL ATOMIC ENERGY AGENCY FOR THE APPLICATION OF SAFEGUARDS”) prevê uma série de possibilidades adicionais de verificações por parte da Agência Internacional de Energia Atômica, provendo maior acesso aos inspetores a locais de desenvolvimentos nucleares e fontes de informação dos países que o implementam. (Disponível em <https://www.iaea.org/topics/additional-protocol> acesso em 3.mar.2021)

Mais recentemente, em 2018, o Presidente norte-americano Donald Trump retirou os EUA do acordo nuclear celebrado com o Irã em 2015[87]. O acordo previa controles mais rígidos ao desenvolvimento de tecnologias nucleares em troca de alívio a sanções econômicas. Em direção contrária, o então Presidente eleito dos EUA em 2020, Joe Biden, já expressava a vontade de reintegrar os EUA ao acordo e expandi-lo para tentar extrair garantias, do Irã, de abandono das pesquisas e desenvolvimentos para armas atômicas[88].

Um ponto adicional do contexto é a postura israelense sobre o desenvolvimento de armas nucleares pelos países da região. O ataque israelense a um reator iraquiano em 1981 demonstrou a disposição israelense em atacar estados rivais que estivessem a caminho de desenvolver armas nucleares. O ataque da Operação Ópera, realizada durante a guerra Irã-Iraque poderia ter se tornado um ponto de inflexão nas rivalidades nucleares, como, por exemplo, na relação entre Índia e Paquistão ao adicionar o ataque preventivo ao leque de opções de medidas contra a proliferação nuclear. Além disso, expôs, na época, as falhas da atuação da AIEA. (KIRSCHENBAUM, 2010)

O ataque israelense ao Iraque não suscitou retaliações e nem gerou mudança significativa na postura de outras rivalidades regionais. Porém, este episódio não pode ser generalizado, já que o Iraque estava com as atenções voltadas para o front de guerra e não possuía outras maneiras de retaliar. Em essência, o ataque gerou algum atrito com os EUA, um aumento da animosidade na região e uma discussão internacional acerca do fato de Israel não ter assinado o acordo de não proliferação[89]. (KIRSCHENBAUM, 2010)

O ataque israelense à um reator na Síria em 2007 pode ser enquadrado na mesma categoria. Israel só admitiu a realização da operação dez anos depois, potencialmente para uso de dissuasão contra os desenvolvimentos iranianos[90].

---

[87] O acordo foi firmado em 2015 e é conhecido como *Joint Comprehensive Plan of Action (JCPOA)*. Ela é oficializada pela resolução 2231 do Conselho de Segurança das Nações Unidas. (disponível em https://undocs.org/S/RES/2231(2015) acesso em 29.jan.2021)

[88] THE ECONOMIST. **Joe Biden wants to re-enter the nuclear deal with Iran.** <https://www.economist.com/middle-east-and-africa/2020/12/05/joe-biden-wants-to-re-enter-the-nuclear-deal-with-iran> Acesso em 06.Dez.2020.

[89] Argumenta-se que o ataque possa ter gerado um esforço redobrado por parte do Iraque para o desenvolvimento de armas nucleares (BRAUT-HEGGHAMMER, 2011), entretanto, Kirschenbaum (2010) argumenta que os esforços despendidos para se manter o desenvolvimento em segredo podem ter impedido seriamente o avanço iraquiano.

[90] REUTERS. **Israel admits bombing suspected Syrian nuclear reactor in 2007, warns Iran**. Disponível em <https://www.reuters.com/article/us-israel-syria-nuclear-idUSKBN1GX09K> Acesso em 02.Fev.21.

3.2.O VÍRUS STUXNET

O principal ataque com o vírus Stuxnet ocorreu em 2009 e 2010. Tratava-se de um vírus especialmente projetado para atacar a estrutura de enriquecimento de urânio em Natanz, no Irã. Este vírus utilizou, pelo menos, quatro vulnerabilidades em sistemas de computador nunca utilizadas antes (*zero day exploits*). O vírus tinha como alvo estruturas de controle industrial, causando efeitos físicos ao manipular as velocidades dos motores de controle. O efeito final do ataque foi a destruição de cerca de 15% a 20% das centrífugas de enriquecimento de urânio do Irã na época.

O contexto da utilização do vírus foi descrito por Zetter (2015). Um ataque cinético tradicional ao Irã não havia ainda sido descartado em meados dos anos 2000, quando a administração Bush iniciou o projeto conhecido como “Operação Jogos Olímpicos”, até hoje não reconhecida oficialmente. A operação tinha como objetivo sabotar a capacidade de enriquecimento de urânio do Irã por meios encobertos, com negação plausível e menores capacidades de retaliação militar por parte do Irã. Os EUA possivelmente contaram com apoio de Israel para o desenvolvimento da arma cibernética.

Embora as instalações em Natanz não fossem diretamente conectadas à Internet, o vírus foi capaz de infectá-la, e até de ser atualizado remotamente em alguns momentos. Uma das especulações iniciais foi de que algum equipamento utilizado por engenheiros havia sido infectado (como um pen-drive). Posteriormente, fontes anônimas teriam reportado que um agente infiltrado holandês, um engenheiro recrutado pela agência de inteligência holandesa, teria implantado o vírus.

O vírus funcionava de maneira escondida. O principal modo de ataque era controlando as velocidades com que as centrífugas atuavam. Aumentando e diminuindo a velocidade de rotação bruscamente foi possível alterar o equilíbrio dos equipamentos, gerando defeitos internos e até mesmo derrubar as centrífugas, destruindo-as no processo e danificando centrífugas adjacentes. Entretanto, a atuação do vírus era bem sofisticada. Para evitar detecção o vírus sabotava as interfaces de controle, mostrando leituras compatíveis com o modo normal de operação, ao mesmo tempo em que alternava entre os modos normais e os modos sabotados ao longo do funcionamento, para evadir as tentativas de análise pelos engenheiros responsáveis. (LANGNER, 2011)

Inicialmente, os engenheiros iranianos acreditaram ser um caso de incompetência[91] ou até mesmo sabotagem interna. Em 2009, o chefe da organização de energia atômica do Irã renunciou após um acidente na usina de Natanz, possivelmente causado pelo vírus.

Uma das características que demonstrou a complexidade e o potencial custo de desenvolvimento do vírus foi a utilização de quatro vulnerabilidades nunca antes utilizadas. Essas vulnerabilidades exploravam falhas de segurança do sistema operacional Windows e permitiam controle com privilégios de administrador nas máquinas infectadas. Além disso, o vírus possuía outras maneiras de se espalhar pela rede local uma vez que a primeira máquina fosse infectada, fornecendo também a capacidade de atualização para versões mais novas depois que um computador da rede estivesse infectado com uma versão mais recente.

A descoberta do vírus se deu por acaso, ao infectar de maneira incorreta computadores fora da usina de enriquecimento que era o alvo. Embora o vírus tenha sido construído com um alvo específico e com salvaguardas para causar danos apenas a ele, tinha capacidade de se espalhar, e, por uma falha dos que o desenvolveram, acabou causando erros e danos colaterais em alguns computadores fora deste alvo. Com isso, analistas e empresas de segurança digital conseguiram exemplos do vírus para estudo e análise.

Análises posteriores demonstraram sua engenhosidade técnica, capacidades e possível custo de desenvolvimento. Uma das características do vírus era sua natureza modular, com estilos de programação diferentes em cada módulo, o que indica uma cooperação técnica de maior escala. Segundo Zetter (2015), os desenvolvedores de cada parte aparentaram ter capacidades técnicas diferentes, sendo esse um dos motivos pela falha do vírus em se manter indetectável em sistemas fora da usina alvo.

3.3.METODOLOGIA PARA O ESTUDO DO CASO

Nesta subseção, serão definidas as hipóteses e variáveis a serem utilizadas como instrumentos para a análise do caso, de maneira a organizar a discussão e os argumentos subjacentes aos eventos demonstrados e conclusões elaboradas. Em outras palavras, objetiva-se uma condução precisa do estudo de caso.

[91] "Eventually, the attacks had another effect: the Iranian scientists suffered low morale, under the impression that they couldn't do anything right; seventy years earlier a bunch of Americans had built an atomic bomb using slide rulers, and they couldn't even get their modern-day centrifuges to work. Overall, Langner likened the Stuxnet effect to the cyber version of 'Chinese water torture.'" (SINGER, 2015, p.83)

Argumenta-se aqui que o caso do Vírus Stuxnet em 2009/2010, é do tipo *most likely case*, onde as características mais emblemáticas de uma categoria deveriam estar presentes para que se aponte na direção de ser, de fato, uma característica do tipo de caso. Esse caso possui as características principais de um ataque militar, onde existiram ganhos estratégicos por um dos lados do conflito, perdas estratégicas pelo outro lado, em conjunto com destruição de ativos militares de uma nação.

Em se tratando de *dissuasão,* o Irã possuía até então capacidade suficiente para que um ataque militar convencional ao seu território pudesse ser retaliado na forma de ataques cinéticos a Israel (ataques militares convencionais com uso de armas como mísseis, tanques, aviões de combate, etc.). Outra forma de dissuasão que o Estado Iraniano empregou foi ameaçar retaliação, elevando, assim, a tensão geopolítica da região. Um ataque cinético tradicional às suas usinas de enriquecimento teria consequências vastas, como o risco de desestabilizar ainda mais o Oriente Médio. Isso se mostrou na relutância dos EUA em acatar os pedidos de Israel para um ataque de modo a interromper o desenvolvimento de armas atômicas pelo Irã.

Caso o incidente se comportasse da mesma maneira de um conflito tradicional, qualquer tipo de ataque poderia ter sido dissuadido por esse contexto. Isso é reforçado pelo fato de que, a despeito das sanções econômicas sofridas por conta de seu programa nuclear e assassinatos de figuras importantes na condução do programa durante o período analisado, o Irã se sentia confiante o suficiente para levar em frente o programa, possivelmente confiando na sua capacidade dissuasória, principalmente em se tratando da capacidade de evitar ações mais impactantes ao programa, como ataques cinéticos.

Entretanto, ao atacar com um vírus de computador, EUA e Israel foram capazes de evitar os potenciais efeitos de uma retaliação; o ataque aparentemente não instabilizou a região e não houve ataques cinéticos convencionais por parte do Irã. Inicialmente a negação plausível sobre a autoria do ataque se mostrou suficiente para que esses efeitos não ocorressem.

O recorte temporal do caso se dará em três etapas: antes do ataque 2003 até 2009, durante o ataque em 2009 e 2010, após o ataque de 2011 a 2015 (um resumo é fornecido na tabela 2). Serão comparadas as estratégias dissuasivas do Irã e dos EUA e Israel, a fim de se entender quais foram os fatores que possibilitaram a expansão do programa nuclear iraniano,

e quais os fatores que possibilitaram o lançamento do ataque cibernético em lugar de um ataque convencional por parte dos EUA e de Israel.

A inexistência de efeito dissuasório em relação aos EUA e Israel após o ataque com o vírus Stuxnet será analisada. A hipótese subjacente, e presente na literatura analisada, é a de que um ataque cibernético pode ser feito com pouca ou nenhuma consequência negativa aos atacantes e que isso acontece mesmo em um contexto em que existe pouca dúvida acerca da autoria (*hipótese h2*). A existência do fenômeno da negação plausível e a demora em estabelecer as cadeias de autoria de ataques são elementos que reforçariam a confirmação desta hipótese.

Um pressuposto importante para esta análise é a questão da existência de custos para qualquer tipo de ataque, além dos evidentes custos monetários de uma operação. Em adição a custos monetários de desenvolvimento e empenho de qualquer artefato militar (seja ele físico, como mísseis ou não físico, como armas cibernéticos) existem custos políticos subjacentes, tanto em termos de política externa como interna. Por exemplo, há a questão da aceitação pelos eleitores locais dos tomadores de decisão e há a possibilidade de sanções internacionais diretas ou indiretas. Além de custos de oportunidade perdidos ao se focar os esforços em determinada ação em detrimento de outras. As consequências negativas advêm de custos *maiores* do que os esperados, consequência positivas, portanto, advém de custos *menores*, ou de benefícios inesperados que compensem os custos.

Indícios no sentido da hipótese *h2* ser positiva apontam para a confirmação da hipótese principal, qual seja, a de que elementos dissuasivos tradicionais não funcionam como dissuasão no contexto de guerra cibernética (*hipótese h1*). Entretanto, a análise em conjunto com os outros casos é necessária para essa confirmação, onde elementos de dissuasão tradicionais poderiam ser identificados.

A ideia de que a quantidade de custos determina a eficácia da dissuasão parte do pressuposto de que a ao se dissuadir deixa-se claro a existência de algum tipo de custo para determinado tipo de ação. Isto é, um ataque será retaliado ao menos na proporção em que o benefício esperado pelo atacante seja menor que o custo imposto pelo defensor. Ou, por outro lado, um ataque terá muito menos efeito no defensor do que o custo de emprego do ataque pelo agressor.

A mera inexistência de consequências negativas *imediatas* para os atacantes não é suficiente para o descarte da ideia de dissuasão, já que as consequências podem advir para

terceiros, ou muito deslocadas no tempo, mas ainda passíveis de análise pelos atacantes. Para o caso analisado, o cálculo dos atacantes neste período provavelmente foi cauteloso, devido à inexistência de exemplos anteriores; o fato do ataque ser conduzido mesmo neste contexto de incerteza adicionaria um elemento para a conclusão da ineficácia da dissuasão tradicional no caso.

Portanto, além dos impactos nos meses subsequentes ao ataque, para o teste da hipótese *h2* será feita análise do contexto da região após a descoberta do vírus, de 2010 até 2015, no período após a descoberta de evidências substanciais da autoria do vírus.

Este caso precisa ser analisado por dois pontos de vista, pela natureza de "via de mão dupla" da dissuasão. Por um lado, o atacante pode ter capacidade para realizar um ataque sem esperar sofrer consequências, e por outro um defensor por ter capacidade de não receber determinados ataques por demonstrar ter capacidade retaliatória suficiente. No caso estudado, os EUA e Israel não utilizaram de armas cinéticas tradicionais para este ataque, o que implica que eles estariam esperando uma retaliação iraniana suficientemente grande caso atacassem nesses termos. Pelo outro ponto de vista, o Irã possuía capacidade dissuasória suficiente para não receber um ataque tradicional, mas não possuía uma projeção suficiente que deixasse claro a um agressor que um ataque cibernético seria retaliado.

Caso os dados apontem no sentido de consequências negativas aos EUA/Israel após a utilização de armas cibernéticas, isso poderia demonstrar um efeito global de redução de utilização futura de ataques com essas armas, principalmente em contextos de instabilidade política. O recurso a ataques por terceiros, neste caso, poderia ser incentivado para desestabilizar oponentes ou contextos políticos. Porém, ainda não há evidências suficientes para conclusões neste sentido, o que pode fortalecer a hipótese de que o ataque poderia ter poucas consequências negativas para o atacante. Ou seja, se um ataque pudesse ter consequências negativas para um atacante, um terceiro ator se utilizaria disso para enfraquecer um inimigo em um contexto de rivalidades expostas. Contudo, a inexistência de casos dessa categoria poderia apontar para a inexistência de consequências graves negativas para o atacante, aumentando a possibilidade de disseminação de ações do tipo, e, consequentemente, fortalecendo a possibilidade de uma situação instável de dominação do ataque.

Tabela 2: Resumo do caso Stuxnet

Evento	Característica
Desenvolvimento de armas atômicas pelo Irã até 2009	Pressões contra o Irã não estavam sendo completamente eficazes, embora houvesse diversas sanções internacionais (incluindo por Estados membros da AIEA).
Ataque tradicional ao Irã	Um ataque tradicional não ocorreu. Capacidades dissuasivas suficientes por parte do Irã.
Ataque cibernético ao Irã em 2009-2010.	Redução da capacidade de enriquecimento de urânio do Irã em quase um quinto. Atrasos significativos no desenvolvimento do programa causados pela destruição das centrífugas e por elementos subversivos adjacentes.
Desenvolvimento de armas nucleares pelo Irã após o ataque cibernético de 2010	Continuação do programa de desenvolvimento de armas nucleares, a despeito dos atrasos sofridos. Novos acordos acerca dos desenvolvimentos nucleares com outros Estados posteriormente.

Fonte: elaborado pelo autor.

Cada variável independente, exposta na tabela 3, será analisada nos três períodos estabelecidos. Algumas variáveis são definidas pela presença ou ausência (*i1, i2, i6*), enquanto outras são definidas pelo aumento, diminuição ou neutralidade (*i3, i4, i5*). Apenas a análise da variável dependente *d2 não* é suficiente para o teste da hipótese *h2*, pois uma consequência dissuasiva importante é o aumento da capacidade dissuasória do outro Estado.

Um aumento ou manutenção da capacidade dissuasória do Irã resulta em *perdas estratégicas* para o EUA/Israel, diminuindo assim sua margem de manobra para controle do contexto político e militar da região (e nesse caso apontando para uma ineficácia das armas cibernéticas), mas não necessariamente *perdas dissuasórias* para EUA/Israel, pois somente a incapacidade de influência no programa nuclear iraniano não implicaria um aumento de punições em potencial ao EUA/Israel, pelo menos em quanto o Irã não finalizasse de fato o desenvolvimento de uma arma nuclear e subsequente capacidade de empenho (e não apenas a continuidade da pesquisa). As perdas em potencial dos atores devem ser analisadas em duas variáveis dependentes separadas, pois, embora não sejam fenômenos completamente independentes, eles se demonstram em sentidos opostos, com elementos diferentes que os caracterizam, a despeito de serem referentes aos mesmos atores. A tabela 3 resume esta análise.

Tabela 3: Quadro para o teste da hipótese h2

Variáveis dependentes (*hipótese h2*)	Variáveis independentes
Capacidade dissuasória do Irã em relação aos EUA e Israel. (Irã não ser punido o suficiente para interromper o programa nuclear) (*d1*)	Presença de ataques convencionais ao Irã (*i1*); presença de ataques cibernéticos ao Irã (*i2*); presença de outras sanções ao Irã (*i3*).
Capacidade dissuasória dos EUA e Israel em relação ao Irã. (EUA/Israel não serem punidos por tentar interferir no programa nuclear do Irã) (*d2*)	Estabilidade política da região (*i4*); Pesquisa de armas atômicas pelo Irã (*i5*); Guerra convencional do Irã a Israel (*i6*).

Fonte: elaborado pelo autor.

A potencial ineficácia das armas cibernéticas, em um *most-likely case*, apontaria na direção de novos desenvolvimentos e modificações de futuras estratégias. As armas cibernéticas estão sendo discutidas e desenvolvidas em diversos países, mas a inexistência de outro caso da magnitude do Stuxnet[92] demonstra o aumento da cautela dos países no emprego dessas armas da mesma maneira. Talvez isso seja produto da maior capacidade de resguardo de segredos de Estado. Entretanto, as consequências estratégicas de um novo ataque dessa magnitude deveriam ser visíveis, e alguma explicação alternativa deveria ser provida caso a caso. Os desenvolvimentos recentes, porém, não apontam nessa direção.

3.3.1. Antes do ataque: 2003 até 2009

A desconfiança da Agência Internacional de Energia Atômica em relação ao programa nuclear Iraniano ganhou força em 2003, após vazamentos de informações sobre a construção da usina de enriquecimento de urânio em Natanz[93]. Segundo Zetter (2015), os inspetores da agência sabiam da existência de material contrabandeado para a produção de urânio enriquecido, assim como de desenhos de centrífugas e peças. Após as inspeções, o Irã aceitou assinar o Protocolo Adicional, em 2003, e se comprometeu em interromper as operações de enriquecimento e reprocessamento de urânio[94].

Entretanto, as capacidades do Irã já estavam avançadas naquele ano. Em relatório do Diretor-Geral da AIEA de 5 de junho de 2020[95], foram reveladas informações sobre a as atividades no período. Aparentemente outras atividades de enriquecimento de urânio foram conduzidas em locais desmontados e higienizados entre 2003 e 2004. Isso aponta uma evidência de que as inspeções da AIEA, e a possibilidade de revelação pública do programa, foram elementos suficientes para diminuição das atividades neste período.

Essa diminuição aponta no sentido de que ações tradicionais, no caso as inspeções e a possibilidade de escrutínio público, possuíam capacidades de diminuir os desenvolvimentos

---

[92] Embora seja possível argumentar que os casos da Ucrânia também possuíram características de sabotagem em larga escala.

[93] No website da AIEA a cronologia das ações relacionadas ao Irã começa em 2002 com a declaração do Irã na conferência geral (Disponível em https://www.iaea.org/newscenter/focus/iran/chronology-of-key-events acesso em 29.Nov.2020). Entretanto, as primeiras inspeções ocorrem em 2003.

[94] INTERNATIONAL ATOMIC ENERGY AGENCY. **Iran to Sign Additional Protocol and Suspend Uranium Enrichment and Reprocessing.** Novembro, 2003. Disponível em https://www.iaea.org/newscenter/pressreleases/iran-sign-additional-protocol-and-suspend-uranium-enrichment-and-reprocessing acesso em 29.Nov.2020.

[95] INTERNATIONAL ATOMIC ENERGY AGENCY. **NPT safeguards agreement with the Islamic Republic of Iran. Report by the Director General.** Junho, 2020. Disponível em https://www.iaea.org/sites/default/files/20/06/gov2020-30.pdf acesso em 29.Nov.2020.

nucleares para fins bélicos. A despeito disso, o alcance e a capacidade da AIEA eram limitados, já que ela de fato não possuía uma agência de inteligência própria, e necessitava conduzir as investigações a partir de informações providas por outras fontes.

A despeito dos avanços gerados pelas inspeções da AIEA, em 2005, com a ascensão ao poder de Mahmoud Ahmadinejad, a retórica anti-Israel e anti-Ocidente ganhou força no Irã. Alguns meses após a eleição as negociações acerca do programa nuclear iraniano foram interrompidas e o Irã voltou a desenvolver o programa. Em fevereiro de 2006 o Irã declarou oficialmente que iria deixar de observar o protocolo adicional e outros procedimentos voluntários de inspeção[96]. Neste ano o grupo de países P5+1 (Reino Unido, Estados Unidos, França, China, Rússia e Alemanha) propôs um acordo ao Irã em troca da interrupção do programa.

Com essa reversão, elevaram-se as tensões entre os principais atores. Por volta de 2006, Israel pressionava os EUA por um ataque cinético às instalações nucleares iranianas, enquanto os EUA temiam que a escalada de ataques levasse a um conflito na região (KAMIŃSKI, 2020). Em julho de 2006, o Conselho de Segurança da ONU adotou resolução requisitando a interrupção do enriquecimento de urânio no Irã e prevendo sanções[97], que foram aprovadas em Resolução de dezembro do mesmo ano[98]. Por volta deste ano, os EUA deram início à Operação Jogos Olímpicos, e, em 2007, houve a utilização da primeira versão de um vírus na usina de Natanz. No entanto, na época, ninguém suspeitou publicamente do propósito do vírus reportado[99].

A existência dessa primeira versão do vírus em 2007 demonstrava a evolução da ideia de um ataque cibernético ao Irã. O desenvolvimento já estava avançado o suficiente para a incursão no sistema e a análise do código do vírus já demonstrava a capacidade de causar danos, embora de maneira diferente da versão que fora colocada em operação dois anos depois. A descoberta desta versão do vírus dá indícios de que as discussões internas dos Estados patrocinadores possam ter sido a causa da demora de seu emprego. Outra causa pode ter sido a espera do momento adequado, em termos de desenvolvimento tecnológicos do Irã

[96] ARMS CONTROL ASSOCIATION. **Timeline of Nuclear Diplomacy with Iran**. Disponível em https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran acesso em 2.jan.2021.
[97] UNITED NATIONS. **Security council demands Iran suspend uranium enrichment by 31 august, or face possible economic, diplomatic sanctions**. Disponível em https://www.un.org/press/en/2006/sc8792.doc.htm acesso em 02.Jan.2021.
[98] [98] UNITED NATIONS. **Security council imposes sanctions on Iran for failure to halt uranium enrichment, unanimously adopting resolution 1737.** Disponível em https://www.un.org/press/en/2006/sc8928.doc.htm acesso em 02.Jan.2021.
[99] ZETTER. **Stuxnet Missing Link Found, Resolves Some Mysteries Around the Cyberweapon**. 2013 Disponível em https://www.wired.com/2013/02/new-stuxnet-variant-found/ acesso em 13.Dez.2020.

ou do impacto máximo da sabotagem técnica e/ou subversão por meio de desmoralização e criação de embates internos entre, de um lado, os controladores e implementadores técnicos, e de outro, os controladores políticos do projeto nuclear iraniano.

A discussão que poderia ser colocada é se a existência dessa primeira versão do vírus em 2007 já poderia ser considerada um ataque cibernético, mesmo sem impactos de sabotagem visíveis. Incursões para espionagem ou para descoberta de informações para o desenvolvimento da arma final não são necessariamente ataques, mas essa primeira versão do vírus possuía a capacidade de causar danos e uma possibilidade é que seu uso não estivesse gerando efeitos suficientes[100] e, por isso, os desenvolvimentos posteriores. Neste caso, a variável relativa à presença de ataques cibernéticos antes de 2009 seria considerada como presente, mesmo que os efeitos não tivessem sido detectáveis.

No final de 2007, o Irã já possuía centrífugas para enriquecer urânio para a construção de bombas nucleares em cerca de um ano de operação de enriquecimento. (CORDESMAN; SEITZ, 2008). Isso gerou forte pressão para uma resposta por parte de Israel e dos EUA, já que a janela para evitar a capacidade de produção de uma arma nuclear estava se fechando.

Em março de 2008, o Conselho de Segurança das Nações Unidas aprovou a Resolução 1803, com mais sanções ao Irã. Em junho do mesmo ano o grupo P5+1 apresentou nova proposta ao Irã de troca de algumas sanções, e impedimento de criação de novas, em troca da interrupção do programa nuclear iraniano.

3.3.2. Durante o ataque: 2009 e 2010

Em junho de 2009 entrou em operação a primeira versão do vírus com capacidade de alterar o funcionamento das centrífugas de enriquecimento de urânio da instalação em Natanz[101]. Nos meses subsequentes, o vírus causou o aumento na perda de centrífugas e permaneceu ativo por cerca de um ano antes de ser descoberto por uma pequena empresa de segurança digital na Bielorrússia, chamada VirusBlockAda, em junho de 2010.

Em agosto e setembro daquele ano os primeiros pesquisadores reportaram publicamente as descobertas acerca do propósito do vírus, ainda sem compreensão total dos

---

[100] COMPUTER WORLD. **New evidence shows Stuxnet used since at least 2007.** Disponível em <https://www.computerworld.com/article/2495609/new-evidence-shows-stuxnet-used-since-at-least-2007.html> Acesso em 29.Dez.2020.

[101] A versão anterior do vírus, de 2007, aparentava ter um método de funcionamento diferente, e aparentemente não foi ativada ou não gerou efeitos suficientemente visíveis.

mecanismos e motivações do ataque. (FARWELL; ROHOZINSKI, 2011). Inicialmente o governo iraniano procurou diminuir a percepção dos danos causados, alegando que apenas computadores pessoais de alguns técnicos haviam sido infectados; entretanto, relatou posteriormente que o vírus estava ativo há pelo menos um ano.

Em novembro de 2010 as operações na usina de Natanz foram encerradas, provavelmente na tentativa de erradicar de vez o Stuxnet. Entretanto, o Irã não explicitou oficialmente o motivo de ter encerrado as operações.

Robin e Baezner (2017) consideram que o efeito imediato do Stuxnet fora o de reduzir as tensões no Oriente Médio, pois, ao diminuir a ameaça imediata do programa nuclear Iraniano também teria diminuído os ímpetos para um ataque cinético convencional ou a necessidade de novas sanções por parte dos EUA e Israel. Também consideram que as estratégias dos países para lidar com ameaças cibernéticas se modificaram após este período. Assim, partindo da análise destes autores, a estabilidade política da região (variável *h5*) teria *aumentado* durante este período. Em adição, a capacidade geral de lidar com ataques cibernéticos teria aumentado para vários países, já que houve incentivos claros para que as políticas de segurança fossem atualizadas após estes eventos.

Esses efeitos sobre a estabilidade regional e a capacidade global de lidar com ataques do tipo podem ser resultados desta demonstração pública de capacidades ofensivas, além do efeito em si da arma cibernética. A utilização *in situ* demonstrou a capacidade de coordenar um ataque dessa magnitude a despeito das salvaguardas e potenciais capacidades defensivas existentes. Esse emprego vai além de um teste de laboratório, como a demonstração da destruição do gerador Aurora em 2007[102], pois demonstra a capacidade de resolver problemas advindos do emprego de arma cibernética em território hostil.

Em se tratando de ataques convencionais ao Irã, uma das possibilidades levantadas por alguns autores (LINDSAY, 2013, BAEZNER; ROBIN, 2017, ZETTER, 2015) é de que a utilização do vírus fora uma estratégia dos EUA para desencorajar um ataque cinético por parte de Israel. Um ataque cinético com o propósito de impedir desenvolvimentos nucleares não seria sem precedentes, já que durante a guerra Irã-Iraque, em junho de 1981 Israel

[102] O teste de destruição do gerador Aurora consistiu de uma demonstração em 2007 acerca da capacidade de um vírus gerar destruição física em um equipamento industrial. (WIRED. **How 30 Lines of Code Blew Up a 27-Ton Generator.** Disponível em https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/ acesso em 10.Jan.2021)

conduziu a operação Ópera, atacando um reator nuclear Iraquiano instalado perto de Bagdá[103]. Caso Israel atacasse diretamente as instalações do Irã, a estabilidade política da região seria duramente afetada, podendo levar a uma guerra. Portanto, a não presença de ataques cinéticos ou guerras neste período também apontaria no sentido de uma maior estabilidade na região.

Por outro lado, os anos de 2009 e 2010 foram caracterizados por dificuldades nas negociações para diminuição do programa de enriquecimento nuclear iraniano[104]. Como consequência destas, na metade de 2010 o Irã começou a sofrer mais sanções. Em junho daquele ano a Resolução 1929 do Conselho de Segurança das Nações Unidas expandiu sanções e sustou o suprimento de sistemas de armas para o Irã. Alguns dias depois, o Congresso dos EUA aprovou novas sanções dirigidas ao setor de energia iraniano. Em sequência, a União Europeia também impôs novas sanções, em diversos setores (ARMS CONTROL ASSOCIATION, 2021).

3.3.3. Após o ataque: 2010 a 2015

Este período é marcado pela negociação entre o Irã e o grupo P5+1. A negociação se alongou por cinco anos enquanto o Irã tentava extrair mais concessões em troca da redução dos desenvolvimentos nucleares e, principalmente, dos estoques de urânio enriquecido a 20%, enriquecimento capaz de fornecer insumos iniciais para a produção de um artefato nuclear.

Entre 2011 e 2014, ocorreram diversas tratativas formais e informais entre o Irã e o grupo P5+1; durante as mesmas, o Irã tentou manobrar para manter a capacidade de desenvolvimento nuclear e reduzir sanções. Em paralelo, algumas das sanções dos EUA e da União Europeia tiveram seu alcance ampliado[105].

Em 2012, o Primeiro-Ministro israelense, Benjamin Netanyahu, em discurso na Assembleia Geral das Nações Unidas, pediu por ações contra o Irã caso o país ultrapassasse a "linha vermelha" de capacidade suficiente para a produção de uma bomba atômica em poucos

[103] Em artigo publicado em 2010, portanto desenvolvido antes do conhecimento público acerca do vírus Stuxnet, Kirschenbaum (2010) analisa a possibilidade de um ataque por Israel às instalações em Natanz, nos mesmos moldes da Operação opera contra o Iraque. A conclusão que o autor chega é a de que não basta uma análise militar para a viabilidade da operação, mas também deve-se levar em consideração a capacidade de reconstrução e reestruturação do programa nuclear do Irã, que em 2010 era muito superior à do Iraque em 1981. Além disso, o autor destaca que, no caso de um ataque cinético, as consequências políticas seriam imprevisíveis.

[104] Em 2009 o grupo P5+1 negocia com o Irã a o acordo de troca de urânio enriquecido a 3,5% por urânio enriquecido a 20% (para uso em produção de energia). Entretanto, o acordo falha em receber aceitação interna. Em 2010, Brasil e a Turquia tentam negociar uma solução com o Irã, mas esta proposta não é aceita pela França, Rússia e EUA. (ARMS CONTROL ASSOCIATION, 2021)

[105] Sanções da União Europeia contra a compra de petróleo iraniano em 2012 e sanções dos EUA contra bancos estrangeiros que mantinham relações comerciais com o Irã em 2011.

meses de desenvolvimento[106]. Durante este período, o governo israelense se manteve cético acerca da efetividade do acordo em inibir o desenvolvimento de capacidades nucleares do Irã[107]. Esta postura de Israel indica certa instabilidade na região; entretanto, um acordo com mais restrições que satisfizesse Israel provavelmente não seria aceito pelo Irã, a despeito das sanções e pressões internacionais a que estava sujeito.

Neste período, o Irã conduziu algumas operações cibernéticas de baixa intensidade contra os EUA/Israel. É possível considerar essas operações como uma espécie de retaliação à utilização do Stuxnet[108]. Estas operações incluíam ataques de negação de serviço (DDOs), espionagem industrial e sabotagem, no caso do ataque à empresa Saudi Aramco (ALSHATHRY, 2016). Em 2012, o Irã instalou o Alto Conselho do Ciberespaço, órgão governamental com objetivo explícito de defesa do espaço cibernético iraniano contra ataques diretos e outras influências ocidentais, utilizando do argumento de defesa contra influências culturais para justificar censuras contra materiais estrangeiros e atos punitivos contra os iranianos que compartilhassem materiais com críticas ao regime. Embora essas ações possam ser encaradas como retaliatórias, não passaram de um limiar de agressão física e provavelmente se aproveitaram de aberturas pontuais geradas por falhas de segurança, ao invés de ataques perpetrados com alta precisão e objetivos claros.

Em 2015, o acordo acerca do programa nuclear iraniano foi finalmente assinado entre Irã e o grupo de países P5+1. O acordo detalhou como se daria a diminuição do crescimento da capacidade de enriquecimento de urânio e as outras limitações para o desenvolvimento do programa nuclear[109]. Em troca as sanções impostas ao Irã seriam suspensas e o país voltaria a ter acesso a fundos internacionais previamente bloqueados[110]. Uma série de fatores pode ter contribuído para a superação dos obstáculos ao acordo; Tarok (2016) lista como um dos fatores o compartilhamento de certos objetivos estratégicos pelos EUA e Irã na região (interesses na Síria, Iraque, Afeganistão, Iêmen), além de um possível sentimento dos

---

[106] UNITED NATIONS. **At UN General Debate, Israeli leader calls for 'red line' for action on Iran's nuclear plans.** Disponível em https://news.un.org/en/story/2012/09/421552 Aaesso em 28.Jan.2021.

[107] **Benjamin Netanyahu Speech to Congress 2015 [FULL]** (vídeo). Disponível em https://www.youtube.com/watch?v=wRf1cdw4IAY acesso em 28.Jan.2021.

[108] Connel (2014) vai além e define que EUA e Israel estariam engajados em um conflito cibernético de baixa intensidade desde 2011. Lindsay (2013) cita os ataques DDOs contra bancos nos EUA e o ataque contra a empresa saudi Aramco como retaliação iraniana e descreve a situação como uma guerra cibernética que dissuasão não conseguiu evitar. ("Deterrence thus failed to stop a cyberwar") Porém, Lindsay também propõe uma explicação alternativa, de que a dissuasão fora eficaz ao limitar as ações retaliatórias ao um campo de baixa intensidade, evitando, por exemplo, ataques cinéticos tradicionais.

[109] Para uma tabela resumo com as principais limitações impostas pelo acordo ver: https://www.armscontrol.org/factsheets/JCPOA-at-a-glance acesso em 04.Fev.2021.

[110] Entretanto, ainda continuaria a sofrer sanções por violações a direitos humanos, entre outras.

tomadores de decisão no Irã de que não haveria uma outra alternativa para redução das sanções econômicas. Maher (2020) argumenta que do ponto de vista do Irã o acordo quebrou um certo "consenso de segurança internacional contra o Irã" em voga nos anos anteriores ao acordo, e por isso o acordo foi oposto por Israel, que recebia benefícios estratégicos deste consenso.

Os desenvolvimentos posteriores foram cada vez menos influenciados pelo ataque com o vírus Stuxnet, e por isso a linha do tempo, para efeitos deste estudo, se detém na assinatura do acordo. Porém, entende-se que os acontecimentos recentes em relação à sua manutenção possam ser fontes importantes de análise para estudos futuros.

3.4.ANÁLISE DAS HIPÓTESES

Nesta seção, as hipóteses serão analisadas de acordo com as variáveis definidas. A tabela 4 resume as variáveis analisadas em cada um dos períodos para cada uma das variáveis dependentes definidas na seção metodológica.

A primeira discussão a ser feita é acerca da publicidade e impacto de ataques cibernéticos. Um possível ataque cibernético não detectado ao Irã em 2007 pode indicar que um ataque cibernético desta escala e com estes objetivos poderia ser ineficaz como ferramenta dissuasória caso o seu propósito e origem ficassem ofuscados. Como o modo de ataque do vírus gerava falhas técnicas que poderiam ser explicadas por erros procedimentais ou por incompetência, apenas falhas muito catastróficas impediriam a continuidade dos desenvolvimentos, já que, a princípio, falhas técnicas poderiam ser sanadas com mais esforços em pesquisas e estudos. Entretanto, um ataque revelado e com propósitos claros demonstraria uma certa propensão à continuidade das tentativas de intervenção, gerando, de fato, efeitos dissuasórios.

Neste sentido, a publicização dos ataques de 2009-2010 seria tanto uma demonstração de capacidade quanto a realização do potencial dissuasório da arma empregada. Então, um ataque cibernético velado em 2007 teria pouco ou nenhum efeito dissuasório, enquanto o ataque de 2009-2010 revelou a disposição para o emprego de ações dissuasórias com potencial destrutivo.

Em se tratando de dissuasão cumulativa, o ataque é uma resposta à continuidade dos desenvolvimentos nucleares, mas a limitação do dano causado poderia apontar a falta do elemento da proporcionalidade, o que indicaria pouca eficácia dissuasória, pelo menos nos

anos imediatamente seguintes. Um esforço maior pelo Irã para compensar as perdas com o vírus pode ter se seguido ao ataque. Entretanto, e a despeito disso, em uma análise em prazo maior, os fatos apontados após 2010 foram no sentido de diminuição dos desenvolvimentos nucleares iranianos, principalmente em se tratando dos acordos assinados em 2015. Porém, estes acordos foram construídos com intervenções de muitos outros atores, e é difícil apontar qual foi o efeito isolado da utilização do vírus.

A hipótese de que um ataque cibernético possa ser feito com pouca ou nenhuma consequência negativa pelos atacantes (hipótese h2) parece se confirmar, levando em consideração o caso Stuxnet e os casos analisados no capítulo 2[111]. Em se tratando de casos com menos publicidade[112], um ataque cibernético pode ser feito e a causa dos danos pode ser atribuída de maneira errônea a qualquer outro motivo, como, por exemplo, incompetência técnica. Por outro lado, um caso com mais publicização e maior certeza de autoria pode até servir como demonstrativo de capacidades do atacante, ou em outras palavras, uma demonstração de força, o que, neste caso, representa uma consequência *positiva* para os atacantes.

A ideia inicialmente desenvolvida foi a de que indícios que apontassem no sentido da hipótese h2 ser positiva levariam a insumos para a confirmação da hipótese principal, que é a de que elementos dissuasivos tradicionais não funcionam como dissuasão no contexto de guerra cibernética (hipótese h1). No caso do Stuxnet, qualquer capacidade que o Irã teve de evitar ataques cinéticos tradicionais não foi capaz de evitar o ataque cibernético. Além disso, qualquer retaliação de parte do Irã envolvendo guerra convencional não foi utilizado após o vírus, o que implica que a resposta tradicional esperada após um ataque cinético, em geral, não aconteceu. Portanto, em termos de dissuasão tradicional, pode-se argumentar que a mesma não é efetiva para evitar ataques cibernéticos.

Entretanto, ao se entender dissuasão sob o paradigma da dissuasão cumulativa, um ataque cibernético seria uma ferramenta de dissuasão ao ser utilizado em resposta a uma ação indesejada dentro de uma análise temporalmente mais longa. No caso do Irã, não é possível

[111] Alguns países foram alvos de sanções pontuais, mas mesmo assim, as consequências não são comparáveis às consequências de um ato bélico tradicional, e ao se pesar as sanções contra os potenciais benefícios, foi demonstrado que houve uma falta de proporcionalidade nos casos anteriores.

[112] Ou com menos escrutínio por parte de empresas de segurança digital. Um dos fatores que tornou possível a análise tão detalhada do Stuxnet foi a atuação dessas empresas nos primeiros meses, com análises forenses que permitiram uma série de deduções acerca de seu propósito e da identidade dos criadores do vírus. O fato de o vírus ter características nunca antes encontradas também deve ter influenciado a quantidade de pesquisadores dispostos a decifrar o funcionamento do seu código, já que ele se demonstrou como um problema de pesquisa interessante.

apontar diretamente que o emprego do vírus tenha levado aos avanços do acordo com o P5+1 em 2015. Porém, a utilização do vírus como resposta aos desenvolvimentos nucleares pode ser modelada como parte de uma estratégia de dissuasão cumulativa. Embora os danos causados diretamente não tenham sido tão grandes, os ganhos por subversão (por exemplo, a confusão causada entre os técnicos da usina) e os ganhos por demonstração de capacidade (demonstrativo de que ações similares poderiam ocorrer no futuro e teriam impactos, o que demonstra que o uso de armas cibernéticas por um adversário deixa de ser apenas especulação) podem ser utilizados como parte de uma estratégia de dissuasão cumulativa mais ampla.

É possível argumentar que a falta do elemento de proporcionalidade, em termos de dissuasão cumulativa, pode ter tornado o ataque pouco eficaz. O dano causado foi moderado, mas, por outro lado, demonstrou a capacidade técnica e a vontade política para o uso de tal tipo de ataque. Um ataque cibernético pode ser, portanto, uma ferramenta dissuasória quando outras ferramentas não se mostrarem eficazes (como sanções econômicas), quando não podem ser utilizadas (como ataques cinéticos contra alvos muito fortificados) ou quando um Estado prefere ficar abaixo de determinado limiar de agressão, como, por exemplo, para evitar uma resposta cinética do defensor.

No caso do Irã, é possível que o Stuxnet tenha evitado uma série de ataques cinéticos e retaliações entre o Irã e Israel. Mesmo em se considerando os ataques cibernéticos vindos do Irã (como o vírus Shamoon utilizado contra a empresa Saudi Aramco[113]) como retaliações, os limiares que demandariam respostas cinéticas não foram atingidos. As análises acima, podem ser resumidas no seguinte quadro abaixo:

[113] NEW YORK TIMES. **In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back.** Disponível em https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html acesso em 01.Nov.2021.

Tabela 4: Resumo das variáveis analisadas

Variável dependente	**Período**	Presença de ataques convencionais ao Irã i1	Presença de ataques cibernéticos ao Irã i2	Presença de outras sanções ao Irã i3	Estabilidade política da região i4	Desenvolvimento de armas atômicas pelo Irã i5	Guerra convencional pelo Irã i6
Capacidade dissuasiva do Irã em relação aos EUA e Israel. (Irã não ser punido o suficiente para interromper o programa nuclear) (*d1*)	Até 2009	Não, mas há pressão de Israel aos EUA no período.	Possivelmente sim, mas não tão impactante.	Aumento das sanções e início das discussões com o grupo P5+1.			
	2009-2010	Não	Sim	Novas sanções no período.			
	Após 2010	Não	Não, ao menos não na mesma escala do Stuxnet.	Discussão gradativa acerca das sanções dentro da discussão do acordo com o P5+1.			
Capacidade dissuasiva dos EUA e Israel em relação ao Irã. (EUA/Israel não serem punidos por tentar interferir no programa nuclear do Irã) (*d2*)	Até 2009				Diminuição da estabilidade com a ascensão ao poder de Ahmadinejad.	Atuação da AIEA interrompe parte dos desenvolvimentos.	Não
	2009-2010				Ligeiro aumento da estabilidade, causado pela redução da capacidade do programa nuclear iraniano.	Afetado negativamente, mas não interrompido.	Não
	Após 2010				Gradual aumento, com o avanço das negociações, mas não linear, com momentos de retração.	Negociações com o P5+1 reduzem a velocidade dos desenvolvimentos nucleares, entretanto, o Irã continua com o desenvolvimento balístico de mísseis de médio alcance.	Não, embora com a presença de algumas ações retaliatórias pontuais no espaço cibernético por parte do Irã.

Fonte: elaborado pelo autor.

3.5.O STUXNET NO CONTEXTO DOS DEMAIS CASOS ANALISADOS

O caso do Stuxnet, embora o mais impactante e emblemático, não ocorreu de maneira isolada aos outros casos estudados. Como demonstrado no capítulo anterior, as possibilidades de ataques cibernéticos já eram aventadas nos anos anteriores e já faziam parte de um certo imaginário político e estratégico-militar nos círculos dos tomadores de decisões.

O Stuxnet se revelou como expressão máxima das possibilidades iniciais de ataques cibernéticos, como uma arma que causa danos físicos e gera destruição, nos mesmos moldes de armas cinéticas, mas com uma precisão muito maior. O ataque ao Iraque em 1981 por parte de Israel gerou os efeitos de redução de desenvolvimentos de armas nucleares, mas em conjunto com a destruição colateral do prédio e a morte de 10 soldados iraquianos e um civil francês. O ataque com o Stuxnet, ao contrário, representou a perda de equipamentos muito específicos, com praticamente nenhum dano colateral. Caso o ataque tivesse ficado velado, os impactos provavelmente não alcançariam repercussão em termos de política internacional e um efeito extra do vírus seria o subversivo, ao causar desconfiança interna e descrédito aos técnicos envolvidos no programa nuclear (já que os efeitos seriam parecidos aos de incompetência técnica, inépcia, imperícia ou até mesmo autossabotagem).

Entretanto, esse ápice das expressões iniciais das possibilidades de vírus de computador como arma teve uma vida curta. Nenhum dos outros casos chegou perto de replicar o potencial do Stuxnet aliado à sua alta precisão e a capacidade técnica demonstrada pelos seus criadores.

Os casos subsequentes demonstraram que a ideia de utilizar armas cibernéticas evoluiu rapidamente. Os custos de desenvolvimento das armas não devem ter se alterado significativamente no período, mas o contexto da sua utilização demandou ciclos de desenvolvimento e uso mais rápidos e mais reativos às mudanças nos contextos políticos e às oportunidades e aberturas identificadas. As interferências russas nas eleições norte-americanas não se apoiaram de maneira significativa em vulnerabilidades em softwares, como os *zero days* utilizados pelo Stuxnet, mas sim em falhas de processos políticos e democráticos, vulnerabilidades humanas em se tratando de influências propagandísticas e falhas regulatórias contra grandes empresas de redes sociais e empresas com acessos a perfis detalhados de usuários. Essas falhas podem ser corrigidas, mas não por uma atualização em um software de computador, mas por atualizações regulatórias, que dependem de processos

políticos mais longos e mais suscetíveis a influências e pressões de ordem doméstica e externa.

Em se tratando de ações de guerra e de ações de dissuasão, o emprego do Stuxnet pode ser entendido dentro do contexto maior da região geográfica e das relações políticas entre os atores envolvidos. O uso do vírus para evitar uma ação cinética por parte de Israel, em conjunto com a capacidade dos EUA de desenvolver e utilizar a arma cibernética, foram fatores que, em conjunto, tornaram este caso possível e único (até agora). Em termos de ações possíveis dentro de um contexto de guerra, demonstraram-se capacidades, como, por exemplo, ataques a dispositivos de controle industrial, que podem ter servido de exemplo para as ações anos depois contra a rede de eletricidade na Ucrânia.

Em se tratando de dissuasão, o Stuxnet evidenciou que a capacidade de evitar ações tradicionais de guerra não se reproduz na capacidade de evitar ações abaixo de determinados limiares de agressividade. O ataque feito com o vírus pode ser entendido como posicionado entre a imposição de sanções e um ataque cinético tradicional, preenchendo assim um "nicho dissuasório" com uma nova opção não presente anteriormente. A possibilidade de ações cibernéticas, desde então, pode ser adicionada ao leque dissuasório de Estados dispostos a investir na pesquisa e desenvolvimento de armas deste tipo.

No próximo capítulo serão analisadas as possibilidades mais recentes, desenvolvidas ou aprimoradas nos anos subsequentes do caso Stuxnet. As relações entre as novas possibilidades e a dissuasão podem alterar significativamente os cálculos dissuasórios dos países. Os novos desenvolvimentos podem ter tornado este caso um ponto único ou podem facilitar o surgimento de casos semelhantes. Isto pode se dar por meio de redução de custos de desenvolvimento e utilização, maior aceitação pelos atores de ataques do tipo ou por descobertas de novos vetores de ataques (ou até mesmo *criação* de novos vetores de ataque, em se tratando de novas tecnologias).

4. DISSUASÃO NO MUNDO PÓS-STUXNET E DESENVOLVIMENTOS FUTUROS

As implicações dos casos estudados vão além dos conflitos cibernéticos analisados. O fim da dicotomia entre "mundo digital" e o "mundo real" se reflete também na perda de sentido da divisão entre uma potencial *diplomacia (exclusivamente) cibernética* e a diplomacia tradicional[114]. Novas reflexões acerca das posturas dissuasivas dos países requerem o entendimento das possibilidades trazidas pelas tecnologias atualmente em uso ou correm o risco de ficarem rapidamente defasadas em relação às ações cibernéticas utilizadas no presente momento por diversos atores. Além disso, as possibilidades fornecidas por tecnologias ainda em desenvolvimento podem adicionar novos vetores de ataque e expor novas brechas de defesa antes não imaginadas, assim como novas capacidades de resiliência e defesas matematicamente robustas em determinados casos.

O objetivo analítico desta seção é adicionar elementos paralelos aos apontados nos capítulos anteriores a fim de entender as implicações para a análise da dissuasão que não foram contemplados apenas pelos estudos de caso, principalmente em prazos mais longos. Pela natureza do tema, parte da discussão é especulativa, porém embasada em indícios apontados pelas pesquisas mais recentes e pela literatura subjacente.

Para este fim, serão estudadas as implicações para a dissuasão que vão além do analisado anteriormente à luz de conflitos cibernéticos, dentro do contexto da evolução teórica do tema. Também serão brevemente analisados os possíveis impactos de desenvolvimentos tecnológicos recentes no campo, como a computação quântica e a internet quântica, assim como os desdobramentos políticos e diplomáticos recentes entre países envolvidos nos casos analisados anteriormente e o impacto do pensamento acerca de operações em domínios múltiplos envolvendo o domínio cibernético e, potencialmente, o espacial. Não há o objetivo de ser exaustivo em relação a todas as possibilidades, já que pela própria natureza do assunto novas tecnologias emergem a todo momento. Entretanto, serão apontadas aqui algumas cujo potencial de modificações impactantes para o tema nos próximos anos é tido como muito expressivo.

[114] Ataffa, Renaud e De Paoli (2020) argumentam, a partir de uma revisão de literatura, que a divisão faz sentido e se reflete em uma dominação do campo pelas áreas mais técnicas em contraposição às áreas de pensamento diplomático tradicionais. Argumenta-se aqui que, pelo menos em relação à segurança internacional, o domínio cibernético já deveria ser entendido em conjunto com as áreas tradicionais, já que seus efeitos são sentidos nelas e diversos países já se utilizam desse domínio para ganhos políticos e projeção de poder.

4.1.DISSUASÃO NO DOMÍNIO CIBERNÉTICO: PASSADO, PRESENTE E FUTURO

A análise dos casos nos capítulos anteriores demonstrou que as capacidades dissuasórias pré-existentes dos países afetados não foram suficientes para impedir uma série de ataques cibernéticos de variadas intensidades. Entretanto, isto não significa que a dissuasão não é relevante no domínio cibernético, mas que ela deve superar o pensamento presente no período da Guerra Fria de que a dissuasão é um caso de "tudo ou nada". Em outras palavras, a ideia de que qualquer ataque represente uma falha dissuasiva não se sustenta ao se analisar os principais casos de ataques cibernéticos das últimas décadas. Neste sentido, o paradigma da dissuasão cumulativa é muito mais esclarecedor, já que permite analisar contextos de aplicação de ações dissuasórias em que ataques de um lado e de outro continuam a ocorrer, mas com intensidades muito abaixo das esperadas pelos analistas que estudaram dissuasão até os anos 90.

Pode-se, então, traçar uma linha do tempo simplificada de evolução das ideias de dissuasão. Em um primeiro momento ela advém de teorias lógicas bem rígidas e estruturadas, em que uma determinada racionalidade dos atores é assumida e o resultado final é a manutenção de um equilíbrio ou a destruição mundial total, sem um meio termo. Em um segundo momento, as teorias abarcam as possibilidades de escaladas e reduções dos conflitos, mas ainda com um horizonte de consequências terríveis. Por fim, com o surgimento da ideia de dissuasão cumulativa, os conflitos podem ser entendidos dentro de uma grande variabilidade de intensidade e ainda serem frutos de estratégias bem-sucedidas (ou malsucedidas) de dissuasão.

A prevalência de diversos tipos de ataques cibernéticos nas últimas décadas sugere então um futuro de ações dissuasórias de diversas intensidades neste domínio. Ações retaliatórias e ações visando a manutenção de determinadas regras de um "jogo" entre rivais podem ser ferramentas comuns no arsenal de possibilidades dos Estados. Aliado às opções disponíveis no meio, a publicidade estratégica dos ataques adiciona uma outra camada de complexidade, ao relacionar um ataque presente ao demonstrativo de capacidades para ataques futuros. Além disso, ações feitas por meio de atores terceiros com negação plausível podem indicar um certo potencial para subversão em larga escala, ao precipitar potenciais conflitos em equilíbrios instáveis.

As armas cibernéticas poderiam ainda apontar para uma situação de prevalência do ataque, onde a defesa é muito mais custosa que o desenvolvimento e a utilização das armas.

Neste caso, as estratégias adotadas pelos países podem ser no sentido de desenvolvimento contínuo de armas e de estratégias de resiliência, isto é, a capacidade de se reestruturar rapidamente após um ataque. Sob os paradigmas de dissuasão mais antigos isto implicaria uma situação instável, com possibilidade de escalada de conflitos (até conflitos cinéticos ou potencialmente trocas nucleares). Porém, sob o paradigma da dissuasão cumulativa, rivais podem estabelecer determinadas linhas de ação a partir das respostas que fornecem em cada etapa do jogo. Por exemplo, um ataque cibernético de baixa intensidade pode ter uma resposta clara com um ataque de média intensidade (cibernético ou não), deixando claro para o agressor que ataques serão respondidos e que essa resposta será, pelo menos, proporcional. Embora esta situação comporte trocas de agressões, ela limita as perdas de cada lado ao longo do tempo. A demonstração de capacidades de resiliência também diminui o alcance dos ataques, desincentivando-os e diminuindo a instabilidade gerada pela situação de preponderância do ataque, mesmo em contextos de dificuldade de construção de defesas sólidas. Em outros termos, trata-se de dissuasão por negação em oposição à dissuasão por punição, ou seja, reduz-se o benefício esperado de um atacante ao invés de aumentar o custo de um ataque.

O contexto de equilíbrio atingido durante a guerra fria, pelo menos entre as grandes potências, tende, a partir da análise construída, a não se manter no domínio cibernético. E as trocas cibernéticas de baixa intensidade entre Rússia, China e EUA demonstram que o equilíbrio entre eles é dinâmico e em constante mudança. Isto aponta para a confirmação da hipótese apresentada no capítulo 1 de que a inexistência de punições tenderia a tornar o espaço cibernético cada vez mais disputado. Porém, deve-se apontar que nos casos analisados não se demonstrou a total inexistência de punições. Elas existiram, em alguns casos, em forma de sanções e possíveis contra-ataques, mas sua eficácia parece ser baixa. Esta ineficácia poderia incentivar punições mais severas a serem testadas pelos atores, buscando efeitos dissuasórios de longo prazo, e aumentando a situação de disputa do espaço cibernético.

No sentido contrário, o medo da escalada dos conflitos poderia manter o atual nível baixo de punições, incentivando ainda mais as ações ofensivas, principalmente ações de subversão e espionagem, em um contexto em que apenas ações de sabotagem poderiam levar a um escalada de um conflito. De qualquer modo, o aumento das ações de subversão nos anos recentes, com consequente baixo número de ações retaliatórias significativas, sugere a manutenção de um equilíbrio dinâmico entre os atores, com predominância de ações ofensivas e desenvolvimentos de capacidades de resiliência (e dissuasão por negação,

consequentemente) em vez de desenvolvimento de defesas robustas (e custosas) ou ações retaliatórias (no mesmo domínio ou em outros).

Por fim, cabe notar o que guia as ações retaliatórias e outras ações dissuasivas dos países envolvidos nos casos. Wilner (2019) argumenta que a prática de dissuasão cibernética ultrapassa muito rapidamente a teoria subjacente. Ao analisar os EUA, Wilner conclui que os documentos que guiam as estratégias de dissuasão e as teorias desenvolvidas pelos acadêmicos estão defasados em relação às práticas de fato do país. Isto poderia indicar que o campo está ainda em pleno desenvolvimento, apontando que mesmo os atores mais profícuos ainda tomam ações guiadas mais pelas experiências pessoais dos tomadores de decisão (incluindo emoções e medos) do que por estratégias coerentes e embasadas em teorias[115]. Os futuros estudos de dissuasão provavelmente serão construídos a partir das práticas correntes, e essas, por sua vez, podem ser modificadas e modificar as teorias mais aceitas de sua época.

4.2.DESDOBRAMENTOS DIPLOMÁTICOS

Em se tratando de diplomacia entre nações, os casos de conflitos cibernéticos por si só tiveram até agora poucas repercussões explícitas de alto impacto. Em casos de sanções por ataques cibernéticos, em geral, apenas alguns indivíduos ou empresas são sancionados, e as consequências para os países em geral tem poucos efeitos dissuasivos de longo prazo[116]. Em termos de consequências diplomáticas por ações no espaço cibernético, cabe-se notar os desdobramentos recentes das relações entre EUA-Israel e Irã, assim como as relações entre a Rússia e a Europa, em particular com os Estados da antiga União Soviética. Outras relações de importância são as entre os EUA e China e mais recentemente, as relações destes dois atores com a Índia.

Por outro lado, devido à natureza da dissuasão ser historicamente ligada à evolução das armas nucleares, é importante notar os desdobramentos diplomáticos também neste campo. As recentes disputas entre EUA e Rússia no caso do Tratado de Redução de Armas

[115] Embora seja possível argumentar que mesmo no auge do apelo das teorias de dissuasão durante a guerra fria essa dinâmica ocorria. Afinal de contas, mesmo quando um dos teóricos mais influentes advogou para um ataque em massa conta a União Soviética isto não ocorreu (felizmente).

[116] Wilner (2019) argumenta que o aumento das sanções na era Obama sinalizou um reforço da postura dos EUA que ações ofensivas no meio cibernético seriam retaliadas, entretanto, é possível argumentar que as sanções a indivíduos e empresas possam ter sinalizado que os países poderiam continuar com essas ações caso possuam outros atores que carreguem a culpa, reforçando o impacto baixo sobre as nações patrocinadoras dos ataques. A diminuição das ações da China em 2015, como apontado no capítulo 2, parece ser uma exceção deste padrão, mas com curta duração.

Estratégicas (New Start[117]) apontam que a questão de redução de armamentos nucleares ainda não deixou de ser utilizada como ferramenta diplomática corrente. A não resolução dos conflitos entre Índia e Paquistão sugere que instabilidades regionais são ainda fatores importantes nos cálculos dissuasórios de diversos países, com aportes subsequentes de outras nações interessadas nas resoluções desses conflitos, no caso, e principalmente, China e EUA. Embora a dissuasão cibernética seja impactada pelas questões de dissuasão nuclear, o oposto não parece acontecer, já que nenhum caso tendo como alvo os países detentores de armas nucleares chegou perto de afetar essas capacidades[118].

4.2.1. Relações EUA/Israel e Irã

Os desenvolvimentos após a assinatura do acordo do Irã com o P5+1 em 2015 não foram lineares no sentido de aproximação iraniana com as potências ocidentais. Desde o início das negociações do Irã com o grupo P5+1, Israel demonstrava oposição às negociações. Nos anos subsequentes ao acordo, o Primeiro-Ministro de Israel fez diversas declarações acusando a potencial ineficácia do acordo e a necessidade de sanções mais severas ao regime iraniano.

As posturas dos EUA e de Israel em relação ao Irã possuem pontos de similaridade e diferenças. Maher (2020) analisa como a preferência dos EUA durante a presidência Obama seria estabilizar a região, contendo as variações do preço do petróleo, utilizando de uma postura de dissuasão bem clara em termos do que uma agressão iraniana representaria como consequência. Por outro lado, Israel advogou, em diversos momentos, em favor de ataques preventivos, para destruição física das capacidades de desenvolvimento nuclear iraniano.

Com a ascensão ao poder de Donald Trump, a agenda dos EUA caminhou para uma convergência maior com Israel. A retirada dos EUA do acordo com o Irã em 2018 reforçou ainda mais essa postura. Com as ações do Irã em resposta à retirada, a capacidade de desenvolvimentos nucleares iraniana provavelmente aumentou no período, aumentando as tensões com Israel e a pressão internacional.

---

[117] *Strategic Arms Reduction Treaty (Start)* assinado em 2010 em continuação à acordos anteriores com objetivos similares.

[118] Pode-se argumentar que os Estados teriam um incentivo para não sinalizarem capacidades amplas de destruição com armas cibernéticas de centros de comando e controle, já que isso demonstraria a capacidade de atacar primeiro e sem consequências. A manutenção dos centros de comando e subsequente manutenção das possibilidades de *second strike* parece ser um fator importante para o equilíbrio nuclear global.

Neste período de desenvolvimentos recentes, a questão da dissuasão cibernética na região reduziu. Nenhuma das trocas de ataques cibernéticos anteriores repercutiu de maneira significativa nas discussões acerca do acordo nuclear ou das ações dos atores na região. Entretanto, não é possível ainda descartar possíveis ações no domínio cibernético na região, ainda mais se combinadas com outros domínios tradicionais de guerra. As negociações e as ações recentes dos atores reforçam posturas muito sólidas construídas ao longo de anos e que requerem ações impactantes para serem modificadas. O emprego de uma arma cibernética atualmente na região provavelmente apenas seria mais uma variável dentro dos cálculos estratégicos atuais e não um motivo de reorganização de posturas, sendo, neste caso, apenas mais uma arma em um domínio específico e não um novo fator de instabilidade.

O acordo recente entre Irã e Rússia na área de defesa cibernética[119] pode adicionar complexidade às relações entre os atores. Embora o acordo esteja voltado para defesa, ele possibilitará acesso da Rússia às variantes capturadas de vírus utilizadas pelos EUA contra o Irã. A análise do Stuxnet foi possível devido à sua dispersão além do alvo original. Entretanto, certas variantes provavelmente ficaram contidas nos sistemas iranianos e não foram compartilhadas abertamente com pesquisadores e outros governos. Com este novo acordo a Rússia passa a ter acesso a mais uma nova fonte de informação acerca das atividades cibernéticas conduzidas pelos EUA e outros atores com interesses na região.

4.2.2. EUA e Rússia

As tentativas de interferência russa nas eleições americanas em 2016 e 2018 não são um fenômeno completamente novo na história americana. Tais tentativas remontam pelo menos ao período da guerra fria e foram construídas ao longo de muitos anos de ações subversivas conduzidas pelos russos. Posard et al (2020) argumentam que a estratégia russa de subversão está baseada em teorias de controle social desenvolvidas na então União Soviética nos anos 60, e aplicadas durante a guerra fria para gerar instabilidade nas nações adversárias. A utilização de redes sociais online e outras ferramentas ampliou o alcance destas ações e possibilitou a confecção de mensagens precisamente direcionadas para grupos específicos, com o objetivo de minar a confiança nos processos democráticos estadunidenses por meio de polarização política da sociedade. Porém, o uso de novas tecnologias isso não

[119] RUSSIAN NEWS AGENCY. **Russia, Iran sign agreement on cyber security cooperation**. Disponível em https://tass.com/politics/1248963 acesso em 26.Jan.2021.

teria alterado de maneira significativa o objetivo subjacente da subversão, mas ampliado seu alcance.

Neste sentido, é interessante notar que a postura diplomática russa em relação ao domínio cibernético mudou na última década (Ford, 2020). No final da década de 90 e anos 2000 a postura Russa era de apoio à promoção de regras globais para o comportamento em relação ao espaço cibernético; entretanto, os EUA não apoiavam essa postura, com receio de que seria utilizada para legitimar tentativas de censura e controles governamentais da Internet. Essa postura inicial se materializou na Resolução da Assembleia Geral da ONU de 1998 (Resolução A/RES/53/70) introduzida pela Rússia a fim de começar as conversas iniciais sobre as ameaças emergentes no espaço cibernético (CHERNENKO, 2015).

A postura inicial da a Rússia advogava pela aplicabilidade da legislação humanitária internacional no meio cibernético, incluindo a aplicação de princípios como a proporcionalidade e necessidade militar em operações cibernéticas. Contudo, mais recentemente essa posição mudou, com o argumento de que é impossível distinguir, de maneira adequada, alvos militares e civis no espaço cibernético (Ford, 2020). Isto é preocupante e alerta para uma postura que aceita a utilização de ataques cibernéticos em ações de sabotagem de larga escala, como a destruição de infraestruturas civis básicas.

A postura inicial dos EUA de tentativa de estabelecimento de canais de comunicação com a Rússia acerca de incidentes cibernéticos, estabelecida em 2013 pelo governo Obama, não impediu as tentativas de influência nas eleições em 2016. Ford (2020) argumenta que a postura inicial não era de dissuasão, mas apenas de comunicação, e que as ações da Rússia não eram meramente um incidente a ser resolvido por canais de comunicação, mas sim uma política deliberada, a ser impedida com ações dissuasivas claras. Entretanto, a falha em fornecer respostas claras às ações russas resultou em novas tentativas de interferência em eleições posteriores, indicando uma falha na postura dissuasiva delineada em 2018 no documento do Departamento de Defesa dos EUA intitulado *Cyber Strategy*. As ações de dissuasão do documento incluíam operações militares em outros domínios como resposta a ataques cibernéticos, mas obviamente isto não aconteceu, tendo como resultado final a falta de credibilidade, sendo assim insuficiente para impedir novas tentativas de ações de subversão cibernéticas da Rússia.

4.2.3. Rússia e restante da Europa

Os casos apresentados no capítulo dois envolvendo a Rússia e países da antiga União Soviética apontam a direção geral da diplomacia russa em relação a esses países – tentativas de reestabelecimento ou manutenção de influência. As ações russas podem ser categorizadas como híbridas, envolvendo aspectos militares e não militares em diferentes graus, de acordo com a capacidade de cada país receptor resistir à sua influência. Os casos da Geórgia e Ucrânia demonstraram a capacidade russa de coordenação em múltiplos domínios, incluindo o cibernético, além de demonstrar a capacidade de ganhos político-estratégicos substanciais da Rússia. Enquanto o caso da Estônia demonstrou que uma ação cibernética pode ser conduzida em um limiar bem mais baixo do que uma ação militar e mesmo assim gerar ganhos políticos ao agressor.

A Rússia foi bem-sucedida em interromper os processos de ingresso à OTAN pela Ucrânia e Geórgia. A anexação da Crimeia pode ser apontada como a culminância de uma série de vitórias russas não contestadas pelas potências europeias e aliados. Um dos principais objetivos estratégicos da Rússia parece ser o de evitar o fortalecimento da OTAN na sua esfera de influência, incluindo países vizinhos.

As ações russas no meio cibernético foram seguidas de sanções leves pela UE e EUA, muitas vezes direcionadas apenas a indivíduos ou empresas[120]. As principais fontes de exportações russas, como gás natural, não foram afetadas e nem a circulação de cidadãos russos no restante da Europa ou EUA. Essa postura leniente aponta à continuidade das ações cibernéticas russas nos próximos anos, talvez com ações mais ousadas nos países de sua esfera de influência. Por outro lado, sanções mais direcionadas às ações russas na Crimeia parecem ter contido o conflito àquela região, o que demonstra a possibilidade de se conter a Rússia[121].

[120] As primeiras sanções contra ataques cibernéticos impostas pela União Europeia só ocorreram em julho de 2020 e foram direcionadas contra seis indivíduos e três entidades. (COUNCIL OF THE EUROPEAN UNION. **EU imposes the first ever sanctions against cyber-attacks**. Disponível em https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ acesso em 28.Mar.2021)

[121] É difícil provar a falta de algo, mas, alguns relatórios apontam a mudança de táticas da Rússia imediatamente após o anúncio das primeiras sanções, e a tentativa de consolidar ganhos rapidamente antes que as negociações começassem. (GALBERT, 2015)

4.2.4. EUA e China

As relações entre EUA e China em termos de diplomacia cibernética ganharam força a partir de meados dos anos 2000, após a descoberta da operação *Titan Rain* e outras ações cibernéticas conduzidas pela China. Em 2015, as conversas bilaterais entre resultaram em uma diminuição verificável de ações chinesas de espionagem industrial no espaço cibernético (BRANTLY; VAN PUYVELDE, 2019). Porém, mais recentemente, a relação entre esses dois atores vem se deteriorando, tendo como principais exemplos as questões da segurança em redes de telefonia 5G, o levantamento de dúvidas em relação à privacidade de dados pessoais de usuários estadunidenses em aplicativos com servidores baseados na China e o controle de exportações de tecnologias de microchips pelos EUA (LEVITE; JINGHUA, 2019).

Em se tratando de objetivos estratégicos e definições destes atores, os EUA e a China são diferentes em pontos cruciais e similares em outros. O entendimento chinês da soberania no espaço cibernético vai de encontro às ideias de liberdade e democracia dos EUA. Por outro lado, ambos entendem a importância econômica da rede e a possibilidade de integração gerada pela Internet nas cadeias de produção globais. Em termos militares, nenhum dos dois está disposto a aceitar restrições para seu desenvolvimento, ao mesmo tempo em que a dependência do ciberespaço gera um sentimento constante de vulnerabilidade em ambos. (XU, 2018)

As ações no espaço cibernético entre China e EUA não são de mão única. A postura dos EUA, então, tenderia a não ser tão extrema, já que existem incentivos claros para a manutenção das próprias capacidades, principalmente em se tratando de monitoramento das capacidades militares por meio de espionagem. As conversas entre Obama e Xi Jinping em 2015 foram claras no sentido de reduzir especificamente a capacidade de espionagem *industrial*, mantendo o status quo restante. Uma continuidade dessa postura é esperada, visto que atende aos interesses dos conglomerados de desenvolvimento industrial dos EUA e à manutenção de uma capacidade quase global de vigilância pelos EUA. Capacidade essa não contestada de maneira sistemática pelas outras potências.

Uma escalada de conflitos entre China e EUA em curto prazo não deveria ser esperada, haja vista a integração das cadeias produtivas dos países. Em se tratando de dissuasão, as comunicações dos EUA no sentido de retaliação em outros domínios a potenciais ataques cibernéticos não são críveis e carecem de exemplos práticos de aplicação. Por outro lado, ações econômicas podem gerar impactos de grande proporção. As recentes

barreiras econômicas erigidas pelos EUA contra o setor de tecnologia da informação chinesa[122] podem, em um prazo maior, diminuir a interdependência em capacidades produtivas no setor de tecnologia da informação[123] por meio de incentivos a pesquisa e desenvolvimento locais, tanto de alta tecnologia por parte da China quanto de capacidade de fabricação local pelos EUA (no fenômeno chamado de *reshoring,* isto é, o retorno da produção para o país original). Isto geraria, potencialmente, um espaço para ações de dissuasão mais críveis e em outros domínios, já que os setores produtivos não dependeriam tanto um do outro. Neste caso, a maior independência das cadeias produtivas poderia representar um fator de instabilidade nas relações entre os dois países, com espaço para ações de retaliação a operações cibernéticas mais robustas. Em adição, o desenvolvimento de tecnologias nativas poderia representar uma maior capacidade de resiliência de ambos os lados, com menos dependência em importações para uma potencial reconstrução, diminuindo os ganhos de um agressor. Tecnologias locais exclusivas também poderiam adicionar elementos defensivos, com disponibilidade menor ou mais controlada, dificultando a pesquisa de vulnerabilidades pelos agressores[124].

4.3.NOVAS TECNOLOGIAS COMO FATORES DE INSTABILIDADE

Conforme novas tecnologias são desenvolvidas e incorporadas às sociedades e aos arsenais dos países, novas possibilidades surgem em termos de ataque, defesa e dissuasão. Os últimos anos viram o crescimento das mídias sociais como vetores de ataque de subversão, e, mais recente, o início do desenvolvimento de respostas defensivas ou de resiliência para esse tipo de ataque, na forma de regulamentações por meio de legislação e ações ofensivas contra grupos perpetradores. Novas tecnologias e novos desenvolvimentos incorporados ao dia a dia das sociedades e ao uso militar terão novos ciclos de exploração de vulnerabilidades e respostas. Algumas destas incluem a computação quântica, a internet quântica, inteligência artificial e aprendizado de máquina, a fragmentação da internet e novas possibilidades de

[122] Barreiras à exportação de maquinário para produção de microchips, componentes básicos para tecnologias e informação e comunicação. (TRT MAGAZINE. **'Chip Wars': US, China and the battle for semiconductor supremacy.** Disponível em <https://www.trtworld.com/magazine/chip-wars-us-china-and-the-battle-for-semiconductor-supremacy-45052> acesso em 28.Mar.2021)

[123] A China destacou em seu plano quinquenal mais recente a importância do desenvolvimento de tecnologias de produção de microchips nacionais. Ainda assim, a capacidade de desenvolvimento de tecnologias de ponta não deve ser atingida em curto prazo.

[124] No caso do Stuxnet, é interessante notar que o que possibilitou a pesquisa de vulnerabilidades pelos desenvolvedores do vírus foi a utilização de componentes fabricados fora do Irã, ainda assim, foi necessário ter uma certeza razoável de quais componentes foram utilizados na usina para que o ataque pudesse ter o efeito esperado.

exploração de vulnerabilidades humanas (como a disseminação de notícias falsas personalizadas em massa). Corridas armamentistas cibernéticas a partir destes desenvolvimentos podem ocorrer em segredo, com pontos de repercussão pública drásticos e repentinos.

Os desenvolvimentos recentes da China no sentido de criação de uma Internet quântica[125] sugerem um futuro de redes mais seguras e com menos possibilidades de interceptação de dados por espiões. A Internet quântica se baseia em princípios físicos que garantem que informações valiosas possam ser transmitidas com a certeza de que, pelo menos na parte quântica, uma interceptação de dados seria detectada. Esta rede seria paralela e não substituiria a internet comum, mas poderia ser utilizada para garantir mais segurança em transações financeiras e redes de transmissão de informações militares.

Por outro lado, o desenvolvimento de computação quântica permitirá a quebra de diversos protocolos de segurança digital atualmente em uso[126]. Protocolos resistentes a essa quebra já foram desenvolvidos e alguns já estão em uso[127], mas muitas das informações já captadas por agências de inteligência e criptografadas atualmente poderão ser decifradas em um futuro próximo[128]. Além disso, a computação quântica permitirá o desenvolvimento de uma gama de novas tecnologias com consequências militares difíceis de prever[129].

A proliferação de agentes privados no desenvolvimento de capacidades cibernéticas tende a tornar o espaço cibernético ainda mais disputado. Conforme empresas de segurança cibernética ganham proeminência e desenvolvem capacidades de atuação competitivas em relação à Estados, as diferenças entre as capacidades dos atores diminuem, adicionando fatores de instabilidade para os cálculos de ataque, defesa e dissuasão dos países. Atores pessoais individuais dificilmente terão alguma proeminência no futuro, já que os desenvolvimentos cibernéticos para fins bélicos requerem grandes investimentos de capital humano e recursos. Porém grandes empresas podem calcular grandes ganhos financeiros em

---

[125] SCIENTIFIC AMERICAN. **China Reaches New Milestone in Space-Based Quantum Communications**. Disponível em <https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/> Acesso em 25.Jun.2020.

[126] Gidney e Ekera analisam como um dos protocolos de segurança hoje considerado muito seguro (RSA 2048 bits) pode ser quebrado com um computador quântico.

[127] O estudo de criptografia pós-quântica (*Post-Quantum Cryptography*) estabelece parâmetros para a criação e utilização de algoritmos em computadores convencionais que são resistentes a quebra por computadores quânticos. (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2021 e BERNSTEIN, 2009)

[128] Embora alguns estudiosos sejam céticos em relação ao quão rápido essas tecnologias serão desenvolvidas. (KALAI, 2016)

[129] Um dos exemplos dado pelo International Institute for Strategic Studies (2019) é o desenvolvimento de radares e sonares quânticos muito mais precisos que os atuais.

adentrar neste tipo de mercado, conforme a utilização deste tipo de arma fica mais comum e aceitável na arena internacional.

Discussões no sentido de dar capacidade legal para empresas utilizarem de técnicas ofensivas (*hack back,* no termo em inglês) para sua própria defesa cibernética foram conduzidas nos EUA nos últimos anos, destacando a proeminência do tema. Porém, as legislações neste sentido ainda não foram aprovadas e ainda há uma certa barreira de aceitabilidade pública e política a ser transposta[130].

A questão da utilização de aprendizado de máquina e futuros desenvolvimentos de inteligências artificiais também podem ser fatores de instabilidade. O aprendizado de máquina (*machine learning*) já é utilizado em diversas ferramentas, inclusive em programas antivírus para detecção aprimorada de vírus nunca antes encontrados[131]. Inteligências artificiais generalistas, entretanto, ainda estão longe de serem desenvolvidas já que a emulação da mente humana é um desafio computacional muito mais complexo. Diversos analistas preveem que a criação de uma inteligência artificial com níveis humanos ainda está a muitas décadas de distância e mesmo os desenvolvimentos mais recentes (como o GPT-3[132]) ainda demonstram que mesmo redes neurais muito grandes ainda não possuem capacidades cognitivas generalistas.

A fragmentação em curso da Internet a princípio poderia apontar para uma segurança maior de redes separadas. Entretanto, os resultados podem variar muito, dependendo de como essa fragmentação ocorrer. Raemdonck (2021) traça um cenário em que a fragmentação da Internet em 2030 faz a rede global se dividir em vários blocos, sem interoperabilidade. Neste cenário a diminuição da cooperação global por inovação e proteção das redes gera espaços para um aumento da espionagem cibernética, mesmo com redes separadas, por meio da diminuição da cooperação global no desenvolvimento de segurança cibernética[133]. Esta

---

[130] O tema é controverso e existem bons argumentos para o impedimento destas ações, como o aumento da instabilidade por meio de uma continuidade de ações ofensivas perpetradas por empresas, fora do controle de governos. Além da dificuldade de se estabelecer limites mínimos (para o início de uma ação) e máximos (de danos causados) nessas abordagens.

[131] Para um exemplo ver Sharma, Krishna e Sahai (2019).

[132] O modelo GPT-3, desenvolvido pelo laboratório de pesquisa OpenAI, utilizou técnicas de aprendizagem profunda para treinar um modelo de rede neural capaz de construir textos muito parecidos com textos feitos por humanos. Essa tecnologia gera novas possibilidades de criação de conteúdos para subversão automatizados, em massa e, potencialmente, muito convincentes.

[133] Por exemplo, pesquisadores de um país A poderiam não ter um acesso fácil ao sistema operacional usado em um país B. Atualmente isso não ocorre, e a comunidade civil de segurança pesquisa vulnerabilidades presentes em sistemas no mundo todo. Caso a disponibilidade seja apenas por meio de furto de informações e espionagem, apenas a comunidade militar poderia ter um acesso contínuo, o que diminuiria muito a pesquisa, e seria focada

fragmentação poderia ocorrer com o aumento da intensidade de ações como o bloqueio dos EUA à utilização de tecnologia americana de chips por empresas chinesas, o que incentivará o desenvolvimento de capacidades locais e substituição tecnológica de componentes chave dos sistemas de rede, possibilitando o desenvolvimento de ecossistemas digitais inteiros não interoperáveis.

4.4.OPERAÇÕES EM MÚLTIPLOS DOMÍNIOS

Como último fator a ser analisado está a prevalência do pensamento estratégico acerca de operações e dissuasão em múltiplos domínios (*cross-domain* e *multi domain*) envolvendo o domínio cibernético. Sweijs e Zilincik (2021) dividem os principais desafios de uma estratégia de dissuasão em múltiplos domínios em dois segmentos: o primeiro como sendo a dificuldade de integração e sincronização presente pela falta de harmonia entre níveis diferentes de guerra nos domínios[134], o segundo se prende à existência de estratégias híbridas utilizando elementos militares e não militares para o alcance de objetivos políticos. Este segundo desafio é o que interessou mais neste estudo, com um exemplo prático analisado no capítulo dois, no caso envolvendo operações simultâneas na Geórgia em 2008.

A dependência das forças armadas modernas em redes de computadores gera uma vulnerabilidade explorável em operações em múltiplos domínios. Atualmente, em um conflito militar, a utilização de armas no domínio cibernético teria como um dos principais objetivos causar efeitos em ativos localizados em outros domínios, como, por exemplo, desabilitar sistemas de operação de baterias antiaéreas[135]. Em se tratando de dissuasão, a postura dos EUA tem sido a de comunicar que ações retaliatórias contra ações no espaço cibernético podem ser respondidas em qualquer outro domínio. Entretanto, esta postura ainda não foi testada. Porém, as respostas possíveis podem ser tão deslocadas do domínio a ponto de não serem críveis como resposta padrão e sim como escalada do conflito, como, por exemplo, uma resposta cinética a bases de operações em resposta a perda de satélites de monitoramento por meio de utilização de armas cibernéticas de um adversário (MANZO, 2011). Neste exemplo, o ator alvo do ataque cibernético poderia justificar a resposta como uma tentativa de manutenção de um equilíbrio de capacidades de monitoramento, mas poderia ser mal interpretado como escalando o conflito.

---

em acúmulo de vulnerabilidades para uso em armas cibernéticas, em vez de divulgação pública para aumento da segurança, como costuma ser no meio civil.

[134] Para uma análise sobre este desafio ver Gady e Stronell (2020).

[135] Nesse caso se tratando de um conflito explícito e não ambíguo.

Gady e Stronell (2020) analisam que os EUA, o Reino Unido e a Alemanha ainda estão no estágio de experimentação em operações em múltiplos domínios envolvendo o domínio cibernético, com cada país tendo desafios diferentes para uma integração crível dos domínios, incluindo questões de legislação interna.

Por fim, estratégias híbridas em domínios múltiplos utilizando elementos não militares complicam ainda mais o cálculo dissuasório. Os ganhos estratégicos e políticos feitos por meios não militares são difíceis de serem dissuadidos com base em poderio militar, já que uma retaliação poderia parecer ainda mais desproporcional e conducente à escalada do conflito. Portanto, um adversário poderia estar conduzindo operações em um domínio tradicional e sofrendo respostas adequadas, enquanto operações simultâneas cibernéticas poderiam estar passando ao largo de uma resposta, e gerando benefícios não contestados para o agressor. Então, mesmo em um contexto de guerra declarada, ataques cibernéticos híbridos poderiam ser incentivados, somando-se aos fatores de instabilidade já discutidos. Um futuro possível seria a aplicação sistemática pelos Estados das ideias de CDD (*cross domain deterrence*), como definida por Gartzke e Lindsay (2019), onde as respostas entre domínios sejam claramente definidas e empenhadas, a fim de garantir a credibilidade à dissuasão. Porém, ainda assim o resultado dessa aplicação não garantiria estabilidade, vistas as características discutidas do meio.

4.5.BALANÇO FINAL: FUTURO DA DISSUASÃO

Os fatores de instabilidade apresentados neste capítulo apontam para um futuro de um espaço cibernético ainda disputado, onde os desdobramentos tecnológicos e os desdobramentos diplomáticos se seguem sem uma barreira clara entre as ações. O emprego de novas tecnologias disruptivas poderá apontar para um futuro de mais dinamicidade de ações governamentais, onde respostas rápidas são dadas a ações ainda não totalmente compreendidas. Ou, por outro lado, caso as tendências atuais se mantenham, respostas muito deslocadas no tempo podem incentivar ações novas e mais ousadas por agressores. A contenção de ataques do tipo sabotagem, principalmente tendo como alvo as grandes potências, impediu a escalada de conflitos, e parece ser uma linha que não será ultrapassada sem consequências. Porém, as ações abaixo deste limiar podem ter efeitos de grande intensidade, gerando significativos ganhos e perdas estratégicas e políticas para os atores envolvidos.

As comunicações de dissuasão que resultariam em escalada significativa de conflitos não parecem ter efeitos, como demonstrado pelas estratégias de dissuasão dos EUA em relação às interferências russas nas eleições. Entretanto, em um paradigma de dissuasão cumulativa, ações mais rápidas e respostas claras a determinados limiares podem ter efeitos dissuasivos importantes ao longo do tempo. De certa maneira, a capacidade dos EUA e das outras grandes potências foi suficiente para evitar ações diretas de sabotagem em suas infraestruturas básicas e militares, contento as ações aos campos de espionagem e subversão.

Em sentido oposto, um futuro de redução da interdependência dos blocos econômicos pode resultar em ações de ataque e retaliação mais ousadas. Atualmente, as ações de retaliação em potencial dos EUA contra a China são muito custosas, já que a economia estadunidense depende da capacidade produtiva da China. Porém, os desenvolvimentos recentes apontam para um futuro de retorno da produção aos EUA e, por outro lado, de desenvolvimento de tecnologias de ponta pela China, diminuindo a interdependência. As ações cibernéticas, neste contexto, podem ter ambições maiores, assim como as ações dissuasivas em resposta.

O mesmo fenômeno ocorre em parte com a dependência da Europa das importações de gás natural da Rússia. No caso europeu, a mudança para matrizes de energia renovável poderia reduzir esta dependência, e permitir ações mais robustas contra as ações russas no ciberespaço europeu.

Em conclusão, o campo parece se encaminhar para equilíbrios dinâmicos, onde novas forças modificam os cálculos dos atores, mas sem mudanças de paradigma completas e reversões abruptas totais. Em resumo, o *Cyber Pearl Harbor* não ocorreu, e não deve ser esperado. A ideia de dissuasão da guerra fria precisa ser abandonada para que as novas possibilidades sejam abarcadas, e a dissuasão cumulativa parece ser o caminho mais viável para manutenção de um equilíbrio, se não imediato, pelo menos em prazos maiores.

CONCLUSÃO

Nesta conclusão serão discutidas as hipóteses identificadas na literatura e apresentadas ao longo desta tese. Em sequência serão apontados os impactos teóricos e conceituais da análise dos casos, à luz do apresentado no primeiro capítulo. Por fim, as perspectivas de longo prazo serão brevemente analisadas, principalmente em se tratando da diminuição da importância dos casos estudados em comparação com as possibilidades e usos mais recentes dentro do domínio cibernético. Em cada seção, os argumentos serão sumarizados e reconstruídos para clareza analítica.

I. HIPÓTESES APRESENTADAS

Três grandes hipóteses foram discutidas ao longo desta. A primeira delas, trata do espaço cibernético como perpetuamente disputado e foi apresentada no primeiro capítulo a partir da argumentação acerca da impossibilidade de dissuasão causada por esta disputa.

A segunda hipótese, presente na análise da literatura empreendida no primeiro capítulo, diz respeito à impossibilidade de dissuasão no domínio cibernético. Diversos dos argumentos menores derivam das características do meio, como, por exemplo, a característica de dominação do ataque no meio, e podem ser analisados dentro dos contextos dos casos estudados no segundo capítulo e no caso do Stuxnet.

Por fim, a última hipótese diz respeito à adição das armas cibernéticas ao leque de opções dissuasivas que um Estado tem a seu dispor. O Stuxnet e os casos envolvendo a Rússia foram elucidativos a esse respeito. Em adição, as ideias mais recentes de diplomacia cibernética nos fornecem insumos para o entendimento de como esses aspectos podem se desdobrar em um futuro próximo.

I.i. Espaço cibernético como espaço disputado

No capítulo 1 foi apresentada a hipótese de que a inexistência de punições para ações no espaço cibernético tenderia a tornar o espaço cada vez mais disputado. Segundo Fischerkeller e Harknett (2017) essa disputa impossibilita a dissuasão por querer impedir atividades em um ambiente de atividades constantes. Entretanto, em vista dos casos analisados, isto não pareceu ocorrer, já que determinados tipos de ação foram dissuadidos, como ações de sabotagem em larga escala. Portanto, o espaço ser permanentemente disputado

não impossibilita a própria existência de capacidade dissuasiva dos Estados, apenas é de se notar que os conflitos neste domínio podem ter variadas intensidades, assim como os conflitos nos outros domínios, e essas intensidades podem resultar diretamente da capacidade de resposta dos atores.

A característica de "atividade constante" presente no meio aumenta a velocidade com que as ações surtem efeitos, e diminui a janela de oportunidade para respostas dos atores. A necessidade de resposta rápida associada à não existência, na prática, dessas respostas, aliada ao medo da escalada de conflitos, se traduz em um domínio turbulento, em que um ataque é difícil de ser compreendido e caracterizado enquanto ocorre. A restrição ao impacto das ações num primeiro momento tem de vir dos agressores devido à impossibilidade de ações defensivas rápidas, e essa auto restrição é baseada no "estoque acumulado" de capacidade de dissuasão do defensor, em termos de dissuasão cumulativa. Portanto, pode-se caracterizar o espaço cibernético como disputado, mas isso, por si só, não impacta a capacidade de dissuasão no meio.

I.ii. Impossibilidade da dissuasão no domínio cibernético

A continuidade dos casos ao longo do tempo e a não contestação em diversos momentos de ganhos políticos ou estratégicos adquiridos por meio de ações no espaço cibernético apontaram para a impossibilidade de dissuasão *stricto sensu.* Porém, resultado contrário parece se apresentar ao se entender os efeitos dissuasivos como cumulativos, já que uma certa restrição à condução de ações mais destrutivas no espaço cibernético foi percebida ao longo da análise dos casos.

Um dos argumentos iniciais presentes na literatura analisada no primeiro capítulo é de que o espaço cibernético poderia ser caracterizado como possuindo a prevalência do domínio do ataque, pela natureza do desenvolvimento das armas cibernéticas. Segundo este argumento, uma vez desenvolvida, uma arma cibernética específica tenderia a ser usada, pois poderia perder sua efetividade rapidamente devido à possibilidade de atualização das brechas nos softwares e hardwares utilizados para empreender o ataque. Entretanto, percebeu-se que a maior capacidade não reside no desenvolvimento de uma arma específica, mas sim na reserva "intelectual" disponível para os Estados, no caso a existência de capacidade de

desenvolvimento, ou seja, a massa crítica conformada por programadores e pesquisadores de segurança em tecnologias de alto nível[136].

Ainda assim, e retomando o argumento da seção anterior, a disputa constante do espaço cibernético aparenta resultar em um meio em que predominam ações de ataque. A dificuldade de respostas rápidas por parte dos alvos é constante, como demonstrado nos casos apresentados em que nenhum ator atingido por ações cibernéticas conseguiu responder rapidamente e à altura. Além disso, as respostas em prazos maiores não pareceram proporcionais aos ganhos dos agressores, sendo pouco eficazes como ferramenta dissuasiva.

Pesando estes fatores, o que sobra de capacidade dissuasiva aos Estados, parece se resumir ao temor da escalada de conflitos, principalmente para outros domínios. Uma escalada possibilitaria ações retaliatórias claras, com destruição de ativos e suas consequências. Ações de sabotagem foram esparsas e contidas no período analisado, embora claramente possíveis, o que leva ao entendimento de que ações de dissuasão no meio cibernético podem impedir uma determinada categoria de ações enquanto possibilitam outras, e, portanto, neste meio, a ideia de dissuasão não pode ser analisada de maneira monolítica.

I.iii. Adição das armas cibernéticas ao leque de opções dos estados

Uma das consequências do surgimento de um novo domínio é a adição ao leque de possibilidades dos Estados. O domínio cibernético vem se consolidando ao longo dos anos como importante palco de operações e os casos analisados demonstram os impactos que as ações neste domínio podem causar. Então, é natural que ações neste domínio sejam também utilizadas para fins dissuasivos. As armas cibernéticas já entram como opções dissuasivas nos documentos de defesa de certos países, como apresentado anteriormente. Entretanto, ainda não parece ter existido um caso claro de retaliação por meio de ações cibernéticas[137].

Umas das características interessantes para a incorporação de armas cibernéticas no leque dissuasório é a capacidade de controle do dano causado. A princípio, o dano de uma arma cibernética pode ser configurado de maneira muito precisa, para atingir exatamente um ativo sem causar danos colaterais substantivos. Alguns casos demonstraram que a imperícia

[136] Capacidades de espionagem poderiam entrar aqui, já que elas permitem o conhecimento dos sistemas específicos em uso pelos alvos, possibilitando certos desenvolvimentos, como, por exemplo, o conhecimento do hardware específicos utilizado nas usinas em Natanz para o desenvolvimento do Stuxnet.

[137] Isso pode ter acontecido no caso do Irã com os ataques patrocinados contra empresas ligadas aos EUA nos anos após o Stuxnet, entretanto, a claridade da comunicação de dissuasão não foi suficiente para caracterizar como tal.

na construção e emprego de uma arma cibernética pode causar danos fora do escopo esperado. Porém, mesmo nestes casos, o dano não foi além de prejuízos econômicos para o alvo e para terceiros.

O caso do Stuxnet pode ser entendido no contexto do emprego de uma ação cibernética com fins dissuasivos[138]. O desenvolvimento de armas nucleares pelo Irã ameaçava os interesses de Israel da região, que, por sua vez, cogitou o emprego de armas cinéticas tradicionais para impedir tal desenvolvimento. O ataque cibernético foi a maneira de atuar diretamente para sustar tal desenvolvimento sem causar outros danos, e a própria contenção do alcance da arma[139] pode ser entendida como um alerta quanto à possibilidade de ações mais impactantes contra o programa nuclear iraniano, mesmo no mesmo domínio cibernético.

II. BALANÇO DOS IMPACTOS TEÓRICOS

As teorias de dissuasão evoluíram de modo muito importante nas décadas da Guerra Fria, como demonstrado no primeiro capítulo. Portanto, é natural que a emergência de um novo domínio impacte o campo de estudo. Algumas questões pendentes voltam a serem analisadas, como a questão da soberania e dos limiares de resposta, ao passo que outras como o significado do que representa uma falha dissuasiva, passam a ser questionados. Aqui serão apresentados alguns dos principais pontos de importância teórica suscitados ao longo do estudo.

II.i. Uma proposta de definição de dissuasão

Retornando às definições iniciais de dissuasão, as discussões apresentas ao longo desta tese reforçam a necessidade de análise feita a partir das escolhas teóricas e conceituais delineadas no primeiro capítulo. Ao se entender dissuasão dentro de um leque de possibilidades de ações agressivas foi possível ir além das análises teóricas emanadas da Guerra Fria para a compreensão de fenômenos impactantes nos tempos atuais. Isso, por si só, não é novo. Mas, o advento do domínio cibernético, possibilitando ações em um campo antes não imaginado e em escalas muito diferentes (com as possibilidades de subversão massiva),

[138] Ou pelo lado da *compellance*, caracterizando a totalidade do caso como um exemplo de diplomacia coerciva.
[139] Em comparação com as possibilidades de destruição apresentadas pela primeira versão não utilizada da arma, descoberta anos depois.

revelou a necessidade de novas abordagem para a dissuasão que permitam uma compreensão eficaz das novas expressões deste fenômeno.

Pode-se comparar o impacto teórico de se entender dissuasão como fenômeno cumulativo às ideias de jogos repetidos da Teoria dos Jogos e à escalada de ações presente no modelo de Powell. Entretanto, as definições iniciais da maioria dos autores analisados focam em *evitar completamente* ataques ou ações agressivas indesejadas, enquanto a dissuasão cumulativa preconiza uma postura de evitar ações *acima de um determinado limiar ao longo do tempo* em um jogo assimétrico e constante. Neste sentido, a ideia de limiares de Powell se mostrou útil como transição entre as ideias iniciais de dissuasão desenvolvidas durante a Guerra Fria e a dissuasão cumulativa, ainda que tal ideia mire à compreensão do momento em que um conflito chega a um ponto sem retorno, com a destruição mútua garantida em um contexto de potências nucleares. Obviamente, a dissuasão aplicada a países não nucleares nunca chegaria a este ponto; em adição, conflitos intermediários envolvendo grandes potências também precisam ser analisados. Segundo o modelo de Powell, a dissuasão não falha quando os Estados caminham em direção ao abismo, mas sim, quando eles ultrapassam o ponto de não retorno nesta caminhada. Em contraposição, a dissuasão cumulativa não implica um ponto de não retorno[140], mas sim o entendimento de que um insucesso dissuasório implica um aumento ou manutenção de intensidade de ações agressivas ao longo do tempo.

A partir da exploração empreendida nesta tese o próprio conceito adotado inicialmente de dissuasão poderia ser então modificado. Portanto, sugere-se a seguinte definição: dissuasão é a capacidade de um Estado de evitar *ou reduzir a intensidade de* ataques ou ações agressivas indesejadas contra si *ao longo do tempo*, recorrendo para tanto, a sua capacidade de resposta, defesa ou resiliência, *dentro de um processo iterativo de comunicação e aprendizado entre os atores*; isto envolve i) a capacidade de impor um custo substancial à outra parte, seja por danos cinéticos, diplomacia ou medidas econômicas e/ou, ii) o custo implicado a um atacante decorrente da capacidade de resistir a ataques substantivos sem grandes danos (dissuasão por negação).

Essa definição abarca as possibilidades de dissuasão cumulativa e suas vantagens práticas em termos de aplicabilidade e utilidade para os Estados em uma moldura ainda comparável com as definições anteriores presentes na literatura. Isto é, os casos anteriores de

[140] Em comparação com *dissuasão nuclear*. Em comparação com outras possibilidades da dissuasão a ideia ainda se aplica, já que as ideias do que representam falhas, isto é, sofrer ações agressivas indesejadas, sejam similares, ainda que o contraste não seja tão grande.

situações em que definições passadas de dissuasão foram aplicados podem ser analisados a partir desta definição proposta, com potenciais ganhos teóricos, em adição a casos novos, que podem ter sido ignorados pela baixa intensidade pontual, mas que façam sentido dentro de uma análise temporal mais longa de trocas entre adversários. A análise que esta definição prescreve é diacrônica, isto é, entende o fenômeno de acordo com sua evolução no tempo, desta maneira sendo possível compreender as questões de aprendizado entre os atores, e como determinadas ações ou falta de ações em momentos chave (isto é, oportunidades utilizadas ou perdidas de definição de regras do jogo) impactaram a magnitude de ações agressivas subsequentes.

II.ii. Soberania no espaço cibernético

A definição acerca da soberania dos países foi desenvolvida ao longo de muitos séculos, e, portanto, parte de ideias que não se traduzem facilmente no espaço cibernético. A própria natureza da rede foi desenhada para evitar controles regionalizados e rotear através de censura e bloqueios. Portanto, advogar por controles regionais e divisão do espaço cibernético faz pouco sentido a partir de suas definições básicas.

Em se tratando da dissuasão no espaço cibernético a soberania está ligada aos problemas de atribuição. Inicialmente, acreditava-se que a facilidade de ocultamento da origem dos ataques cibernéticos poderia representar a impunidade quase total dos perpetradores. Entretanto, nos casos mais impactantes é possível analisar quem obtém ganhos com a ação e quem deteria os meios e motivos para um determinado ataque. No caso do Stuxnet, diversos vazamentos de informação também foram cruciais para a redução da dúvida quanto à autoria. Ainda assim, as análises forenses necessárias para garantir a certeza da autoria terminam se somando à letargia das respostas.

Alguns países pretendem garantir um determinado nível de soberania em seu espaço cibernético, como a China. Entretanto, o custo econômico de uma desconexão e controle total da rede seria muito alto. Diante disso, as barreiras impostas devem ter um nível de "porosidade" alto, o que impede, de fato, que a China possa clamar por soberania total em seu espaço cibernético.

Portanto, argumenta-se aqui que é praticamente impossível clamar por soberania no espaço cibernético como solução para qualquer um dos desafios atinentes a esse espaço apresentados nesta tese, à (improvável) exceção de um país que se mostre disposto a arcar

com as graves consequências de se desconectar da rede global. Em termos práticos, resulta que qualquer nível de soberania dependente de "controles de fronteiras" não será um fator importante para o controle do meio, e não deveria entrar como fator em um cálculo dissuasório dos países.

II.iii. Comunicação de dissuasão e credibilidade

As comunicações relacionadas à dissuasão são apresentadas de diversas maneiras. A mais comum se refere aos documentos públicos de defesa publicados pelos países, em que menções à dissuasão como objetivo são, em geral, diretas. Entretanto, mesmo nestes documentos verificou-se que não são expressas de modo claro as eventuais respostas a ataques cibernéticos. Há, por vezes, referências a potenciais respostas em outros domínios, mas nada específico em se tratando de ataques cibernéticos bem definidos.

Outros tipos de atividades tem o potencial de comunicar de maneira mais clara e gerar mais credibilidade do que os documentos de defesa, como o demonstram algumas das ações examinadas nos casos apresentados. Como exemplo emblemático foi apontado o ocorrido na Ucrânia em dezembro de 2016, quando um ataque sofisticado foi direcionado a poucos alvos, com o que se dava a conhecer uma capacidade específica, impactante e crível, em adição à disposição de empregá-la.

O domínio cibernético permite então aproximações e distanciamentos interessantes no que respeita à comunicação e à credibilidade em contextos de dissuasão, em relação às práticas das grandes potências durante a Guerra Fria. Por um lado, e ao contrário das armas nucleares, as armas cibernéticas são constantemente empregadas. Por outro lado, é possível traçar um paralelo entre ataques cibernéticos restritos e a credibilidade decorrente de capacidades evidenciadas por testes nucleares, embora um teste nuclear em si diga muito pouco sobre a disposição de emprego[141].

A autocontenção em um ataque pode ter então um papel comunicativo e de conferir credibilidade à dissuasão, o que pode ser assim resumido: "se eu posso fazer ação X contra *este* ativo Y, então eu posso fazer a ação X contra *todos* os seus ativos Y, portanto não faça a ação que me desagrada W". Isso pode apontar um futuro de ações muito sofisticadas, mas

[141] Mas pode-se argumentar também que a utilização em campo de armas cibernéticas muito sofisticadas, porém contidas, também diga pouco sobre a vontade de utilização em larga escala. Ainda assim, a utilização de armas cibernéticas é claramente mais comum e corriqueira que a utilização de armas nucleares.

com poucos alvos, onde os papéis estratégicos e comunicativos podem se confundir em níveis fundamentais.

II.iv. Escalada de conflitos

As ideias iniciais sobre escalada de conflitos presentes na literatura sobre dissuasão levavam os conflitos a um extremo muito rapidamente, com a destruição nuclear sempre possível. Entretanto, com o modelo construído por Powell (1990), os degraus de um conflito podem ser analisados sem levar a um resultado matemático de troca nuclear inevitável. Com o advento das armas cibernéticas mais degraus podem ser adicionados à escada, já que elas permitem uma dosagem mais precisa do dano causado. Além disso, ações que antes eram consideradas separadas se misturam, isto é, aos danos físicos são adicionadas as categorias de subversão e espionagem, dentro de um mesmo "pacote" de desenvolvimento de armas cibernéticas.

A mistura das categorias de sabotagem, espionagem e subversão adiciona complexidade aos cálculos dissuasórios. Um ataque do tipo sabotagem pode resultar danos econômicos significativos, similares até a um lançamento de um míssil contra um ativo. No entanto, a imaterialidade da arma aliada ao risco quase nulo (até agora) de perda de vidas[142], faz com que uma resposta em outro domínio, mesmo que com impactos econômicos similares, pareça desproporcional e servindo ao propósito de escalar o conflito.

Uma ação de espionagem raramente implicaria uma resposta em outro domínio. Tradicionalmente os países aceitam determinado nível de espionagem entre si; porém, a questão que se coloca é sobre como proceder quando, com ferramentas cibernéticas, é possível realizar espionagem em um nível muito mais massivo. Além disso, a espionagem para fins militares (inclusive o desenvolvimento de armas cibernéticas mais precisas) e para ganhos econômicos se misturam.

Quanto ao aspecto de subversão, pode ser traçado um paralelo com as ações tradicionais de propaganda, que em geral não suscitariam respostas militares. Entretanto, se antes era necessário infiltrar de alguma maneira os canais de comunicação em massa de um rival, hoje com as ferramentas online é possível atingir uma parte significativa de um país com campanhas de informação falsas. Uma resposta proporcional parece se conter no campo

[142] Obviamente, determinados ataques podem causar danos suficientes para causar mortes, como, por exemplo, um ataque a uma rede de energia elétrica que deixe os hospitais sem eletricidade por um período prolongado. Entretanto, esse efeito seria bem óbvio e calculável pelos atacantes e não um resultado somente colateral.

diplomático e econômico, mas nos casos analisados isso não pareceu suficiente para dissuadir os agressores.

Até agora, nenhum conflito pareceu escalar de maneira significativa a partir de um ataque cibernético. O ocorrido parece apontar na direção contrária, isto é, ataques que aparentemente deveriam ter sido retaliados não o foram, ao menos não na proporção esperada. Portanto, fica a questão: como reagir adequadamente a um ataque cibernético sem oferecer uma resposta com possibilidades de escalada do conflito? Como se vê na próxima seção, e argumentado ao longo desta tese, o paradigma da dissuasão cumulativa oferece uma resposta.

II.v. Dissuasão cumulativa

A questão da dissuasão cumulativa provém da pergunta inicial sobre o que representa, de fato, uma falha dissuasiva. Em contextos de atores não nucleares[143], as ideias de destruição mútua não fazem sentido. Portanto, limiares menores de dissuasão precisam ser definidos. A transposição dessas ideias para o campo cibernético suscita ações e contrarreações, com regras que podem ser definidas pelos participantes do "jogo" a partir da postura adotada em cada etapa.

Como visto nos casos apresentados, um ataque cibernético dificilmente terá resposta à altura e com a rapidez necessária. Entretanto, mesmo uma resposta tardia, porém com comunicação clara acerca do objetivo dissuasivo, poderia ter o potencial de definir a regra do jogo, caso aplicada de maneira coerente e constante. As respostas tomadas em conjunto e contra atores muito específicos e, em geral, atores meramente operativos, não se mostraram suficientes, o que potencialmente indica um caminho de necessidades de respostas mais bem elaboradas, contra atores decisórios (atores políticos) dentro de uma moldura de atuação constante e bem definida. Ainda assim, o resultado a ser esperado desta postura não seria a ausência de ataques, mas sim ataques menores e menos impactantes nas trocas futuras.

Em resumo, o argumento final é que não se deve encarar cada troca cibernética como falha da capacidade dissuasiva de um país, tanto em termos de análise teórica quanto em termos de ações práticas de um determinado Estado. A falha é representada pela continuidade de ações agressivas com a manutenção ou o aumento de intensidade dos ataques. Em adição, entender cada ataque cibernético sofrido como uma falha na capacidade de dissuasão sugeriria

[143] Ou no contexto de atores nucleares claramente não dispostos a utilizar armas de destruição em massa, o que parece razoável supor acerca de praticamente todos os atores detentores de armas nucleares desde a segunda Guerra Mundial.

um futuro de constantes falhas dissuasivas sem escalada de conflitos, o que seria contraintuitivo ao se tentar entender o fenômeno pelo prisma das teorias tradicionais de dissuasão. Pelo lado das ações práticas dos Estados, falhas constantes representam a necessidade de uma mudança de comportamento para o seu enfrentamento; entretanto, a ausência dessa mudança indicaria a falta de alternativa prática. A alternativa, neste caso, poderia ser a aplicação de dissuasão cumulativa.

É possível que o futuro se desenvolva de forma diferente, e um ataque cibernético resulte em uma escalada de conflito repentina. Isto poderia acontecer caso uma das tecnologias disruptivas apresentadas no quarto capítulo seja totalmente dominada por um ator disposto a usá-las antes que outros atores desenvolvam respostas adequadas. Entretanto, os principais países responsáveis pelo desenvolvimento dessas tecnologias já possuíram tecnologias novas e disruptivas em diversos momentos, e mesmo utilizações em ataques cibernéticos não resultaram em escaladas significativas de conflitos, como visto no período de cerca de vinte anos apresentado nos casos.

A adição de armas cibernéticas ao leque de possibilidades de dissuasão permite ainda maior controle sobre ações retaliatórias, como visto anteriormente. Em se tratando de dissuasão cumulativa essas opções poderiam ser utilizadas dentro do entendimento da criação de regras de jogo. Um dos problemas iniciais no domínio era o entendimento de que a criação de armas cibernéticas seria esporádica e fruto de oportunidades representadas pela descoberta de falhas ocasionais em softwares e hardwares. No entanto, a capacidade contínua de desenvolvimento de certos países demonstra que isso não é o caso, o que implica que o desenvolvimento de armas cibernéticas pode ser algo comum no arsenal dos países e, portanto, disponível permanentemente como opção.

Por fim, encarar a dissuasão como fenômeno *cumulativo* outorga certa prescritividade à teoria. Isto é, ela sugere como os países deveriam se portar para acumular capacidade dissuasiva e reduzir os impactos de ataques sofridos. Ao longo desta tese foram apontados pontos em que uma ação com objetivos de dissuasão cumulativa poderia ter sido produtiva, e momentos em que a falha em se utilizar destas oportunidades resultou em perdas concretas. Isto é exemplificado no caso da Ucrânia, em que falhas de resposta resultaram em ataques ocorridos em sequência, sem consequências significativas para os atacantes, e, portanto, sem definições claras de regras de engajamento que poderiam resultar na diminuição da intensidade dos ataques ao longo do tempo.

Um ponto contrário à utilização da teoria, em termos de construção de fato de políticas de segurança, é a possibilidade de aceitação da instabilidade advinda de constantes trocas de agressões. Embora a perspectiva de redução de intensidade de longo prazo se mantenha, a análise de o quão longo é esse prazo ainda seria necessária. E a discussão que permaneceria seria a de quanto tempo seria razoável esperar pelos efeitos de dissuasão cumulativa antes que ela fosse considerada bem ou malsucedida nas aplicações práticas.

III. REDUÇÃO DA IMPORTÂNCIA DOS CASOS EM PERSPECTIVAS DE LONGO PRAZO

Os casos considerados emblemáticos vão se modificando ao longo do tempo. Vários dos eventos aqui apresentados eram inéditos em seu tempo e sua compreensão foi objeto de muitas discussões. Entretanto, mesmo aqueles eventos mais impactantes tendem a ter sua importância reduzida ao longo do tempo, e, no caso do domínio cibernético, este tempo pode ser muito rápido devido ao desenvolvimento de novas tecnologias e novos entendimentos. O caso da Estônia em 2007 e o Stuxnet são exemplos de casos que atraíram muita atenção e estudo nos anos subsequentes, mas que foram perdendo importância, tanto devido ao esgotamento de informação quanto aos impactos mais relevantes de casos posteriores. As próximas seções analisam a diminuição da importância desses dois casos. Há de se notar que o conjunto de casos analisados, a despeito de uma possível obsolescência, se prestaram à validação teórica desenvolvida nesta tese, ainda mais em se tratando de um fenômeno com um número relativamente reduzido de ocorrências.

III.i. Estônia

Os ataques sofridos pela Estônia em 2007 foram intensos durante o período da ação, embora fossem simples de um ponto de vista técnico[144]. A inação inicial da OTAN deu lugar ao reconhecimento da importância do tema com a instalação do CCDOE e posterior desenvolvimento da primeira e segunda edição do Manual de Tallin. O impacto de um ataque cibernético patrocinado por um Estado foi perdendo importância com a normalização de ações do tipo, além da crescente e significativa sofisticação de que se revestiram desde então. Os impactos de longo prazo na Estônia passaram pelo aumento da segurança cibernética do

[144] Nenhuma arma sofisticada foi desenvolvida para o ataque, a ferramenta que possibilitou as ações de DDOS era uma comum e já tinha sido utilizada em outras ações.

país, além de terem alimentado intensa discussão no restante dos países da OTAN. E, em adição, a ocidentalização da Estônia afastou cada vez mais a possibilidade de a Rússia vir a exercer influência naquele país com qualquer nível de legitimidade.

III.ii. Stuxnet

A capacidade demonstrada pelo vírus Stuxnet foi surpreendente à época. Porém, e desde então, outros casos revelaram capacidades comparáveis (como as ações cibernéticas contra a Ucrânia) ou em escalas muito maiores (como a influência da Rússia nas eleições estadunidenses). Outro fator de redução da importância do caso foi a não continuidade de ações semelhantes nos anos seguintes. Ou seja, o mesmo representou um ponto isolado interessante, mas não foi precursor ou paradigmático de ações de sabotagem cibernética de grande complexidade patrocinadas por Estados, mesmo depois do transcurso de mais de uma década.

O avanço das tratativas acerca do acordo nuclear com o Irã também apontou no sentido de uma diminuição do impacto do vírus. O acordo foi elaborado e assinado alguns anos depois do caso, a despeito das ações dos EUA e Israel terem tido o potencial de modificarem os termos das negociações.

IV. PERSPECTIVAS FUTURAS

Ao contrário de casos específicos, a segurança entre países dificilmente perderá importância nas próximas décadas, e o entendimento dos fenômenos novos que a afetam terá de ser atualizado em um ritmo muito mais intenso do que no século passado. O domínio cibernético é o mais recente, porém nada indica que que novos domínios possam ainda vir a existir, embora, por agora, qualquer discussão nesse sentido seja meramente especulativa.

A dissuasão não deixará de ser perseguida e praticada, não importando qual seja compreensão sobre como se dará, já que, muito além de um fenômeno próprio do campo da segurança internacional, a dissuasão é parte do repertório do comportamento *humano*. Seres humanos desenvolvem práticas dissuasivas em diversos campos. O campo de segurança internacional exibe a vantagem de ser aquele no qual o fenômeno é mais extensamente estudado, além da psicologia e da criminalística.

Por fim, enquanto países detiverem armas nucleares será muito difícil desvencilhar qualquer discussão acerca da segurança internacional deste fato. As décadas posteriores à Segunda Guerra Mundial demonstraram que, mesmo sem o emprego de armas nucleares, o efeito de sua própria existência não pode ser ignorado. Mesmo que chegássemos um dia à conclusão de que, olhando para trás, nenhuma arma nuclear nunca teria sido utilizada de fato, não poderíamos assumir isso para o futuro, pois não parecer haver capacidade maior inerente o ser humano do que a capacidade de surpreender.

REFERÊNCIAS BIBLIOGRÁFICAS

ACÁCIO, I. e SOUZA, G. **Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço?** Anais do 36º Encontro Anual da ANPOCS, 2012.

ACTON, J. M. Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. **International Security**, v. 43, n. 1, p. 56–99, ago. 2018.

ADAMS, J. Virtual Defense. **Foreign Affairs**, v. 80, n. 3, p. 98, 2001.

ALDRICH, R. W. **The international Legal Implications of Information Warfare.** Colorado Springs: Institute for National Security Studies, 1996. Disponível em <http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf> Acesso em 10.jul.2016.

ALPEROVICH, D. **Towards Establishment of Cyberspace Deterrence Strategy**. 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.) CCD COE Publications. Tallinn, Estonia, 2011. Disponível em <https://www.ccdcoe.org/uploads/2018/10/TowardsEstablishmentOfCyberstapeDeterrenceStrategy-Alperovitch.pdf>. Acesso em 20.jul.2019.

ALSHATHRY, S. Cyber Attack on Saudi Aramco. **International Journal of Management & Information Technology**, v. 11, n. 5, p. 3037–3039, 30 dez. 2016. Disponível em <https://rajpub.com/index.php/ijmit/article/view/5613/pdf>. Acesso em 13.maio.2021.

APPLEGATE, S. D.; STAVROU, A. **Towards a Cyber Conflict Taxonomy**. 5th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn, 2013. Disponível em <http://www.ccdcoe.org/publications/2013proceedings/d3r1s2_applegate.pdf>. Acesso em 10 ago.2016.

APPLEGATE, S. D. **The Dawn of Kinetic Cyber.** Center for information Systems, 2013. Disponível em <https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf>. Acesso em 10.out.2019.

ARMS CONTROL ASSOCIATION. **Timeline of Nuclear Diplomacy With Iran.** Disponível em <https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran>. Acesso em 12.jan.2021

ARQUILA, J. Can information Warfare ever be Just?**. Ethics and Information Technology**, v. 1 (3), p. 203-212, 1999. Disponível em <http://philpapers.org/rec/ARQCIW>. Acesso em 10.ago.2016

ARQUILLA, J. et al. (EDS.). **In Athena's camp: preparing for conflict in the information age**. Santa Monica, Calif: Rand, 1997. Disponível em: <https://www.rand.org/pubs/monograph_reports/MR880.html>. Acesso em 12.fev.2020.

ATTATFA, A.; RENAUD, K.; PAOLI, S. D. Cyber Diplomacy: A Systematic Literature Review. **Procedia Computer Science**, v. 176, p. 60–69, 2020.

AYSON, R. **Thomas Schelling and the nuclear age: strategy as social science**. London: Cass, 2004.

BAEZNER, M. e ROBIN, P. **Hotspot Analysis: Stuxnet.** CSS Cyber Defense Project. Center for Security Studies, Zurich. 2017. Disponível em <https://www.researchgate.net/publication/323199431_Stuxnet>. Acesso em 10.jan.2021.

BENDIEK, A.; METZGER, T. **Deterrence theory in the cyber-century: lessons from a state-of-the-art literature review.** Working Paper RD EU/Europe. 2015. Disponível em <https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf>. Acesso em 10.ago.2016.

BERNSTEIN, D. J. et al. **Post-quantum cryptography**. Berlin: Springer, 2009. Disponível em <https://link.springer.com/chapter/10.1007/978-3-540-88702-7_1>. Acesso em 13.Maio.2021.

BRAMS, S. J.; HESSEL, M. P. Threat Power in Sequential Games. **International Studies Quarterly**, v. 28, n. 1, p. 23, mar. 1984.

BRANTLY, A. **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.** American Foreign Policy Interests, v. 36, n. 5, p. 334–335, 3 set. 2014.

BRAUT-HEGGHAMMER, M. Revisiting Osirak: Preventive Attacks and Nuclear Proliferation Risks. **International Security**, v. 36, n. 1, p. 101–132, jul. 2011. Disponível em <www.jstor.org/stable/41289690>. Acesso em 1.Fev.2021.

CASTELLS, M. **The Internet galaxy: reflections on the Internet, business, and society**. Oxford ; New York: Oxford University Press, 2001.

CHEN, J. **Does conventional deterrence work in the cyber domain**? ECCWS 2018 17th European Conference on Cyber Warfare and Security. 2018.

CIOFFI-REVILLA, C. A Probability Model of Credibility: Analyzing Strategic Nuclear Deterrence Systems. **Journal of Conflict Resolution**, v. 27, n. 1, p. 73–108, mar. 1983.

CHERNENKO, E. et al. Russia's Cyber Diplomacy. **Hacks, Leaks and Disruptions: Russian Cyber Strategies,** Popescu, N.; Secrieru, S.(eds.), European Union Institute for Security Studies (EUISS), 2018, pp. 43–50. Disponível em <www.jstor.org/stable/resrep21140.8>. Accesso em 27 Mar. 2021.

COLBY, E. A. Why nuclear Deterrence is Still Relevant. **Thinking about Deterrence: enduring questions in a Time of Rising Powers, Rogue Regimes, and Terrorism.** Pag. 82. Air Force Research Institute, 2013.

CONNELL, M. **Deterring Iran's Use of Offensive Cyber: A Case Study.** (Relatório) CNA Analysis & Solutions. 2014. Disponível em <https://apps.dtic.mil/dtic/tr/fulltext/u2/a617308.pdf>. Acesso em 13.maio.2021.

CORDESMAN e SEITZ. **Iranian Weapons of Mass Destruction: Iran's Nuclear Weapons Programs: Work in Progress?** CSIS – Center for Strategic and International Studies. 2008. Disponível em <https://csis-website-prod.s3.amazonaws.com/s3fs-

public/legacy_files/files/media/csis/pubs/081106_iranwmdnuclear.pdf>. Acesso em 5.jan.2021.

CRAIG, G. e EKERÅ, M.. **How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.** 2019. Disponível em <https://arxiv.org/abs/1905.09749>. Acesso em 01.abr.2021.

DELPECH, T. **Nuclear deterrence in the 21st century: lessons from the Cold War for a new era of strategic piracy**. Santa Monica, CA: RAND, 2012. Disponível em <rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1103.pdf>. Acesso em 23.out.2021.

DEMCHAK, C. C. e DOMBROWSKI, P. J. Rise of a Cybered Westphalian Age: The Coming Decades. **The Global Politics of Science and Technology**, v. 5(1), p. 31-62 Springer. 2014.

ERNEST, D. C. The Gardener and the Craftsmen. **World Politics at the edge of Chaos: Reflections on Complexity and Global Life,** p. 32. 2015.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **Post-Quantum Cryptography: Current state and quantum mitigation**. 2021. Disponível em <https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation>. Acesso em 14.maio.2021.

FIREEYE. **Special Report | Double Dragon: Apt41, A Dual Espionage and Cyber Crime Operation.** 2019. Disponível em: <https://content.fireeye.com/apt-41/rpt-apt41/>. Acesso em 21.ago.2020.

FORD, C. A. International Security in Cyberspace: New Models for Reducing Risk. **Arms Control and International Security Papers**, v. I, n. 20, 2020. Disponível em <https://www.state.gov/wp-content/uploads/2020/10/T-paper-series-Cybersecurity-Format-508.pdf> Acesso em 21.nov.2021.

FARWELL, J. P.; ROHOZINSKI, R. Stuxnet and the Future of Cyber War. **Survival**, v. 53, n. 1, p. 23–40, fev. 2011.

FIELD, A. Schelling, von Neumann, and the Event that Didn't Occur. **Games**, v. 5, n. 1, p. 53–89, 25 fev. 2014.

FISCHERKELLER, M. P.; HARKNETT, R. J. Deterrence is Not a Credible Strategy for Cyberspace. **Orbis**, v. 61, n. 3, p. 381–393, 2017.

FORTMANN, M.; HLATKY, S. **The Revolution in Military Affairs: Impact of Emerging Technologies on Deterrence.** IT. Paul, P. Morgan & J. Wirtz (Ed.), Complex Deterrence (pp. 304-320). 2009. Chicago: University of Chicago Press. Acesso em 20.out.2019.

GADY, F.; STRONELL, A. **Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030**. CCDCOE. 2020. Disponível em < https://ccdcoe.org/uploads/2020/12/8-Cyber-Capabilities-and-Multi-Domain-Operations-in-Future-High-Intensity-Warfare-in-2030_ebook.pdf> Acesso em 21.nov.2021.

GALBERT, S. DE. **A year of sanctions against Russia -- now what? a European assessment of the outcome and future of Russia sanctions: a report of the CSIS Europe Program**. Center for Strategic and International Studies. 2015.

GAMERO-GARRIDO, A. M. **Cyber Conflicts in International Relations: Framework and Case Studies.** 2014. Disponível em: <https://ssrn.com/abstract=2427993>. Acesso em 14.fev.2021.

GARTZKE E.; LINDSAY J.R. **Cross-Domain Deterrence: Strategy in an Era of Complexity.** Oxford University Press; 2019. Disponível em <https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190908645.001.0001/oso-9780190908645>. Acesso em 24.jul.2021.

GEER, D. **Cybersecurity as Realpolitik**. (conferência) Black Hat USA, 2014. Disponível em <http://geer.tinho.net/geer.blackhat.6viii14.txt>. Acesso em 10.ago.2016

GEERS, K. **Cyberspace and the Changing Nature of Warfare**. Centre of Excellence Tallin, Estonia. OTAN. 2008. Disponível em <http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf>. Acesso em 10.ago.2016.

GELINAS, R. R. **Cyberdeterrence and the problem of attribution**. Tese (mestrado em Estudos de Segurança). Georgetown University, Washington D.C. 2010. Disponível em < https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/historical/gelinasRyan.pdf> Acesso em 21.nov.2021.

GREENBERG, A. **Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers**. First edition ed. New York: Doubleday, 2019.

GUERRERO-SAADE, J. A.; RAIU, C.; MOORE, D.; RID, T. **Penquin's Moonlit Maze: The dawn of Nation-State Espionage**. Ed.: Kaspersky Lab e King's College. London, 2017. Disponível em <https://kas.pr/4P8E>. Acesso em 23.ago.2020.

HAGEN, A. **The Russo-Georgian War (2008): The Role of the cyber attacks in the conflict.** AFCEA. 2012. Disponível em <https://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf>. Acesso em 11.maio.2021.

HAGESTAD, W. T. **21st century Chinese cyberwarfare: an examination of the Chinese cyberthreat from fundamentals of Communist policy regarding information warfare through the broad range of military, civilian and commercially supported cyberattack threat vectors.** Ely, Cambridgeshire, Reino Unido: IT Governance Publishing, 2012.

HAIZLER, O. The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking**. Cyber, Intelligence, and Security**, V. 1, No. 1, 2017. Disponível em <https://www.inss.org.il/wp-content/uploads/2017/03/The-United-States%E2%80%99-Cyber-Warfare-History-Implications-on.pdf> Acesso em 23/out.2021.

HAMDOUNI, H. **The digital destruction: A case study of Stuxnet within the theory of new and old wars.** Suécia: Swedish defense University. 2017. Dispoínvel em <

https://www.diva-portal.org/smash/get/diva2:1141887/ATTACHMENT01.pdf> Acesso em 23.out.2021.

HARTMANN, K.; GILES, K. **The Next Generation of Cyber-Enabled Information Warfare**. 2020 12th International Conference on Cyber Conflict (CyCon). **Anais**... In: 2020 12TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (CYCON). Estonia: IEEE, maio 2020. Disponível em: <https://ieeexplore.ieee.org/document/9131716/>. Acesso em: 18.dez. 2021

HILDRETH, S. A. **CRS Report for Congress: Cyberwarfare**. Estados Unidos: The Library of Congress, 2001. Disponível em <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-014.pdf>. Acesso em 17.out.2021.

IASIELLO, E. **Cyber Attack: A Dull Tool to Shape Foreign Policy**. 5th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2013 Disponível em <http://www.ccdcoe.org/publications/2013proceedings/d3r1s3_Iasiello.pdf>.Acesso em 20.jul.2016.

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. **The military balance. 2019: [the annual assessment of global military capabilities and defence economics].** London: Routledge for The International Institute for Strategic Studies, 2019.

ISIKOFF, M.; CORN, D. **Russian roulette: the inside story of Putin's war on America and the election of Donald Trump**. First edition ed. New York: Twelve, 2018.

JAMIESON, K. H. **Cyberwar: how Russian hackers and trolls helped elect a president: what we don't, can't, and do know**. New York, NY: Oxford University Press, 2018.

JERVIS, R. Cooperation under the Security Dilemma. **World Politics**, v. 30, n. 2, p. 167–214, jan. 1978. Disponível em <http://www.sscnet.ucla.edu/polisci/faculty/trachtenberg/guide/jervissecdil.pdf>. Acesso em 20.jul.2016.

JERVIS, R. Deterrence Theory Revisited. **World Politics**, v. 31, n. 2, p. 289–324, jan. 1979.

JERVIS, R. Rational Deterrence: Theory and Evidence. **World Politics**, v. 41, n. 2, p. 183–207, jan. 1989.

JERVIS, R. **American foreign policy in a new era**. New York: Routledge, 2005.

KALAI, G. The Quantum Computer Puzzle. **Notices of the American Mathematical Society**, v. 63, n. 05, p. 508–516, 1 maio 2016.

KAMIŃSKI, M. Operation "Olympics Games." Cyber-sabotage, as a tool of American intelligence aimed to counteract the development of Iran's nuclear program. **Security and Defence Quarterly**, v. 29(3), p.63-71, 3 jun. 2020.

KAPLAN, F. M. **Dark territory: the secret history of cyber war**. New York: Simon & Schuster, 2016.

KAVALSKI, E. (ED.). **World politics at the edge of chaos: reflections on complexity and global life**. Albany: State University of New York Press, 2015.

KELLO, L. **The Virtual Weapon and International Order.** New Haven; London: Yale University Press, 2017. Disponível em <http://www.jstor.org/stable/j.ctt1trkjd1>. Acesso em 20.out.2019

KIRSCHENBAUM, J. Operation Opera: an Ambiguous Success. **Journal of Strategic Security**, v. 3, n. 4, p. 49–62, dez. 2010. Disponível em <https://scholarcommons.usf.edu/jss/vol3/iss4/8>. Acesso em 30.jan.2021.

KREPINEVICH, A. F. **Cyber warfare, a "nuclear option".** Center for Strategic and Budgetary Assessments. 2012. Disponível em <http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/>. Acesso em 20.jul.2016.

LANGNER, R. Stuxnet: Dissecting a Cyberwarfare Weapon. **IEEE Security & Privacy**. v. 9, no. 3, pp. 49-51, Maio-Jun 2011.

LANGNER, R. **The Stuxnet History** (vídeo e transcrição). 2020. Disponível em <https://www.langner.com/2020/07/the-stuxnet-story/>. Acesso em 13.dez.2020

LAWSON, S.; MIDDLETON, M. K. Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. **First Monday**, 1 mar. 2019. Disponível em <https://firstmonday.org/ojs/index.php/fm/article/view/9623/7736>. Acesso em 22.Set.2020.

LEVITE, A. e JINGHUA, L. **Relations in Cyberspace: Toward Collaboration or Confrontation?** China Military Science. 2019. Disponível em < https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213> Acesso em 21.nov.2021.

LIAROPOULOS, A. **War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory.** Procedings of the 9th European Conference on Information Warfare and Security. University of Macedonia: Thessaloniki. Grécia, Julho 2010. Disponível em <https://www.academia.edu/292652/War_and_Ethics_in_Cyberspace_Cyber-Conflict_and_Just_War_Theory_in_9th_European_Conference_on_Information_Warfare_and_Security_University_of_Macedonia_and_Strategy_International_Thessaloniki_Greece_1-2_July_2010>. Acesso em 20.jul.2016.

LIAROPOULOS, A. **Deterrence in Cyber Space: Implications for National Security.** MICS Yearbook. Mediterranean Council for Intelligence Studies. 2012. Disponível em < https://www.researchgate.net/publication/264327596_Deterrence_in_Cyber_Space_Implications_for_National_Security> Acesso em 20.nov.2021.

LIBICKI, M. C. **Cyberdeterrence and cyberwar**. Santa Monica, CA: RAND, 2009.

LIBICKI, M. C. **Expectations of Cyber Deterrence.** Strategic Studies Quarterly. Winter edition, 2018.

LIBICKI, M. C. **Correlations Between Cyberspace Attacks and Kinetic Attacks**. 2020 12th International Conference on Cyber Conflict (CyCon). **Anais**... In: 2020 12TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (CYCON). Estonia: IEEE,

maio 2020. Disponível em: <https://ieeexplore.ieee.org/document/9131731/>. Acesso em: 18.nov.2021

LINDELAUF, R. **Nuclear Deterrence in the Algorithmic Age: Game Theory Revisited.** OSINGA F.: SWEIJS T. (eds) NL ARMS Netherlands Annual Review of Military Studies 2020. NL ARMS (Netherlands Annual Review of Military Studies). T.M.C. Asser Press, The Hague. 2021. Disponível em <https://link.springer.com/chapter/10.1007/978-94-6265-419-8_22>. Acesso em 10.out.2021.

LILLY, B.; CHERAVITCH, J. **The Past, Present, and Future of Russia's Cyber Strategy and Forces**. 2020 12th International Conference on Cyber Conflict (CyCon). **Anais**... In: 2020 12TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (CYCON). Estonia: IEEE, maio 2020. Disponível em: <https://ieeexplore.ieee.org/document/9131723/>. Acesso em: 18.nov.2021

LIN, H. Cyber conflict and international humanitarian law. **International Review of the Red Cross**, v. 94, n. 886, p. 515–531, jun. 2012.

LINDSAY, J. R. Stuxnet and the Limits of Cyber Warfare. **Security Studies**, v. 22, n. 3, p. 365–404, jul. 2013.

LINDSAY, J. R.; GARTZKE, E. (EDS.). **Cross-domain deterrence: strategy in an era of complexity**. New York, NY: Oxford University Press, 2019.

LINDSAY, J. R.; CHEUNG, T. M. **From Exploitation to Innovation: Acquisition, Absorption, and Application in China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.** Oxford University Press. 2015.

LITSCHKO, I. **Lights Out: An Examination of Cyber Attacks in Ukraine And The Baltic States**. The Mackenzie Institute, 2017. Disponível em <https://mackenzieinstitute.com/2017/10/lights-out-an-examination-of-cyber-attacks-in-ukraine-and-the-baltic-states/>. Acesso em 13.set.2020.

LOWTHER, A. (ED.). **Thinking about deterrence: enduring questions in a time of rising powers, rogue regimes, and terrorism**. Maxwell Air Force Base, Alabama: Air University Press, Air Force Research Institute, 2013. Disponível em <https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0133_LOWTHER_THINKING_ABOUT_DETERRENCE.pdf> Acesso em 20.nov.2021.

MAHER, N. Balancing deterrence: Iran-Israel relations in a turbulent Middle East. **Review of Economics and Political Science**, v. ahead-of-print, n. ahead-of-print, 14 mar. 2020.

MALLORY, K. **New Challenges in Cross-Domain Deterrence**. Santa Monica, CA: RAND Corporation, 2018. Disponível em: <https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE259/RAND_PE259.pd> Acesso em 15.ago.2021.

MANDIANT. **APT1: Exposing One of China's Cyber Espionage Units.** (Relatório). 2013. Disponível em <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>. Acesso em 02.set.2020

MANZO, V. **Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?** Strategic Forum. National Defense University. 2011.

MAZARR, M. J. **Understanding Deterrence.** Rand Corporation. Disponível em <https://www.rand.org/pubs/perspectives/PE295.html>. Acesso em 12.out.2021.

MEARSHEIMER, J. J. The Case for a Ukrainian Nuclear Deterrent. **Foreign Affairs**, v. 72, n. 3, p. 50, 1993. Disponível em <www.jstor.org/stable/20045622>. Acesso em 19.out.2019.

MORGAN, P. M. **Deterrence now**. Cambridge [England] ; New York: Cambridge University Press, 2003.

NACITA, I.; REITH, M. Cyber War and Deterrence: Applying a General Theoretical Framework. **Air & Space Power Journal**, v.30, p. 74-83, 2018. Disponível em <https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-30_Issue-4/2018_4_10_nacita_s_eng.pdf >. Acesso em 20.jan.2019.

NACHT M, SCHUSTER P, URIBE EC. **Cross-Domain Deterrence in American Foreign Policy**. In: GARTZKE, E., LINDSAY, J. R. Cross-Domain Deterrence: Strategy in an Era of Complexity, New York: Oxford University Press, 2019. Oxford Scholarship Online, 2019.

NEUMANN, J. von e MORGENSTERN. **Theory of Games and Economic Behavior**. Princeton: Princeton University Press, 1953.

NYE, J. S. Deterrence and Dissuasion in Cyberspace. **International Security**, v. 41, n. 3, p. 44–71, jan. 2017. Disponível em: <https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf>. Acesso em 15.ago.2021.

O'CONNELL, M. E. Cyber Security without Cyber War. **Journal of Conflict and Security Law**, v. 17, n. 2, p. 187–209, 1 jul. 2012. Disponível em <http://jcsl.oxfordjournals.org/content/17/2/187.full.pdf>. Acesso em 20.jul.2016

PAUL, T. V.; MORGAN, P. M.; WIRTZ, J. J. **Complex deterrence: strategy in the global age**. Chicago: University of Chicago Press, 2009.

PETALLIDES, C. J. **Cyber terrorism and IR Theory: Realism, Liberalism and Constructivism in the New Security Threat.** Inquiries Journal, v. 4(03). Disponível em <http://www.inquiriesjournal.com/a?id=627>. Acesso em 09.ago.2016.

POSARD, M. et al. **From Consensus to Conflict: Understanding Foreign Measures Targeting U.S. Elections**. Santa Monica, CA: RAND Corporation, 2020. Disponível em <https://www.rand.org/pubs/research_reports/RRA704-1.html>. Acesso em 14.fev.2021.

POTEETE, A. R.; JANSSEN, M.; OSTROM, E. **Working together: collective action, the commons, and multiple methods in practice**. Princeton, N.J: Princeton University Press, 2010. Disponível em <https://www.researchgate.net/publication/49956255_Working_Together_Collective_Action_The_Commons_and_Multiple_Methods_in_Practice_A_Poteete_MA_Janssen_E_Ostrom>. Acesso em 14.nov.2021.

POWELL, R. **Nuclear deterrence theory: the search for credibility**. Cambridge; New York: Cambridge University Press, 1990.

RAEMDONCK, N. van. What If… The Internet Is No Longer Open? **What if...not? The cost of inaction,** European Union Institute for Security Studies (EUISS), LU: Publications Office, 2021.

SCHELLING, T. C. **The strategy of conflict**. 8. print ed. Cambridge, Mass: Harvard Univ. Pr, 1981.

SCHMITT, M. Classification of Cyber Conflict. **Journal of Conflict and Security Law**, v. 17, n. 2, p. 245–260, 1 jul. 2012.

SCHMITT, M. N.; NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (EDS.). **Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence**. Cambridge ; New York: Cambridge University Press, 2013.

SCHNEIDER, J. G. **Deterrence in and through Cyberspace.** GARTZKE, E., LINDSAY, J. R. Cross-Domain Deterrence: Strategy in an Era of Complexity, New York: Oxford University Press, 2019.

SCHWARTAU, W. **Information Warfare: Chaos on the Electronic Superhighway.** New, York, USA: Thunder's Mouth Press. 1994

SHARMA, KRISHNA E SAHAI. **Detection of Advanced Malware by Machine Learning Techniques.** Arxiv (preprint). 2019. Disponível em <https://arxiv.org/abs/1903.02966> Acesso em 14.maio.2021.

SINGER, P. W. **Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons.** Case W. Res. J. Int'l L. 79, v.47, 2015. Disponível em: <https://scholarlycommons.law.case.edu/jil/vol47/iss1/10> Acesso em 14.fev.2021.

SNYDER, G. H. Deterrence and power. **Journal of Conflict Resolution**, v. 4, n. 2, p. 163–178, jun. 1960.

SNYDER, G. H**. Deterrence and Defense: toward a theory of National Security**. Princeton, NJ: Princeton Univ. Press, 1961.

SOESANTO, S. **Trend Analysis: The Evolution of US deterrence strategy in Cyberspace (1988-2019)**. Center for Security Studies (CSS), ETH Zürich, 2019.

SPERANDEI, M. Bridging Deterrence and Compellence: An Alternative Approach to the Study of Coercive Diplomacy. **International Studies Review**, v. 8, n. 2, p. 253–280, jun. 2006. Disponível em <http://www.jstor.org/stable/3880225> Acesso em 19.out.2019.

SWEIJS, T., e ZILINCIK, S. The Essence of Cross-Domain Deterrence. **NL ARMS Netherlands Annual Review of Military Studies 2020**, pp. 129-158. TMC Asser Press, The Hague, 2021.

TADDEO, M. **An Analysis For a Just Cyber Warfare.** 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2012 Disponível em <http://www.ccdcoe.org/publications/2012proceedings/3_5_Taddeo_AnAnalysisForAJustCyberWarfare.pdf>. Acesso em 20.jul.2016.

TAROCK, A. The Iran nuclear deal: winning a little, losing a lot. **Third World Quarterly**, v. 37, n. 8, p. 1408–1424, 2 ago. 2016.

TERTRAIS, B. How relevant is Nuclear Deterrence today. **Nação e Defesa**, v. 140, p10-24, 2018. Disponível em <https://comum.rcaap.pt/bitstream/10400.26/23984/1/TERTRAISBruno_p10_26.pdf> Acesso em 20.jul.2019.

TOR, U. 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. **Journal of Strategic Studies**, v. 40, n. 1–2, p. 92–117, 2 jan. 2017.

VAN PUYVELDE, D.; BRANTLY, A. F. **Cybersecurity: politics, governance and conflict in cyberspace**. Cambridge, UK ; Medford, MA, USA: Polity Press, 2019.

WILNER, A. S. US cyber deterrence: Practice guiding theory. **Journal of Strategic Studies**, v. 43, n. 2, p. 245–280, 23 fev. 2020.

WILSHUSEN, G. C. **Cybersecurity: Threats Impacting the Nation.** Testimony Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives. United States Government Accountability Office. 2012. Disponível em <http://www.gao.gov/assets/600/590367.pdf> Acesso em 20.jul.2016.

WILSON, W. The Myth of Nuclear Deterrence. **The Nonproliferation Review**, v. 15, n. 3, p. 421–439, nov. 2008.

WIVES, W. W. **Situações de conflito no uso da Internet: embates e soluções.** Dissertação (mestrado em Ciência Política), Brasília, Universidade de Brasília, 2013.

XU, P. **Nine Areas of Disputes in the Debate on International Cyber Norms**. China Institute for international Strategic Studies. 2018. Disponível em < https://ceipfiles.s3.amazonaws.com/pdf/CIISS_Nine+Areas+of+Dispute+in+the+Debate+on+International+Cyber+Norms+-+full.pdf> Acesso em 21.nov.2021.

ZAGARE, F. C. Rationality and Deterrence. **World Politics**, v. 42, n. 2, p. 238–260, jan. 1990. Disponível em <http://www.jstor.org/stable/2010465>. Acesso em 09.out.2021.

ZETTER, Kim. **Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.** Broadway Books; Reprint edition. 2015