Software Power

Um Olhar Brasileiro

Marcelo Malagutti

INSTITVTO VEGETIVS

Para mais informações sobre esta publicação visite
www.vegetius.org.br/lv2022-02

ISBN: 978-65-997420-1-9

Publicado pelo Instituto Vegetius, Brasília, DF, Brasil

Malagutti, Marcelo
Software power : um olhar brasileiro / Marcelo Malagutti. -- Brasília, DF : Instituto Vegetius, 2022.

ISBN 978-65-997420-1-9

1. Brasil. Forças armadas 2. Ciberespaço - Aspectos políticos 3. Defesa nacional 4. Informação eletrônica governamental 5. Sistemas de segurança 6. Software 7. Software - Desenvolvimento 8. Tecnologia da informação - Aspectos sociais - Brasil I. Título.

22-104550 CDD-355.033081

O Instituto Vegetius é uma instituição brasileira, de caráter filantrópico, sem finalidades lucrativas e sem qualquer vinculação política ou partidária, que atua na área social mediante a realização de pesquisas, estudos, análises e ações voltadas a auxiliar na melhoria de políticas públicas e tomada de decisão e no engajamento da sociedade nos temas de defesa nacional, segurança nacional e internacional, guerra e paz, relações entre forças armadas e sociedade, ciência e tecnologia no âmbito da defesa e segurança nacionais e internacionais, geopolítica e relações internacionais, planejamento, estratégia, estudos estratégicos e ciências militares em geral.

As publicações do Instituto Vegetius não necessariamente refletem as opiniões de seus clientes e patrocinadores.

Se você gostar deste livro, apoie o Instituto Vegetius!

Faça uma doação por meio do PIX.

www.vegetius.org.br

CONVENÇÕES TIPOGRÁFICAS

As seguintes convenções tipográficas podem afetar a compreensão do texto, devendo ser percebidas da seguinte forma:

- ‘Aspas simples’ são usadas em transcrições, realces ou uma citação dentro de uma citação.
- “Aspas duplas” marcam o início e o fim de uma citação que não exceda cinco linhas inteiras; citações de texto em notas de rodapé; expressões vernaculares usadas apenas em um ambiente profissional específico; termos relativos, como gíria, apelidos ou um significado irônico; ou definições conceituais de termos.
- *Itálico* destaca títulos de livros, periódicos, peças de teatro, filmes, óperas, música, pinturas e esculturas. Nomes de espécies científicas, palavras, expressões e frases em outros idiomas (incluindo latim) citados no texto a ser enfatizado também podem estar em itálico.
- **Negrito** realça os nomes dos capítulos, seções e subseções, e letras ou palavras quando o uso de qualquer um dos métodos mencionados acima não for possível.
- <u>Sublinhado</u> indica os nomes das subseções.

Em conformidade com a norma ABNT NBR 6024, a numeração progressiva é utilizada para os trechos do nível um (seções primárias, ou capítulos) ao nível cinco (ex .: 1.1.1.1.1.).

SUMÁRIO

Página intencionalmente deixada em branco.

1. Prelúdio

Pode o "*Software Power*" (Poder de Software) ser uma ferramenta de coação e de dissuasão entre estados nacionais? Esta é a questão respondida neste livro, que concluiu que boas capacidades de software podem ser usadas tanto para compelir nações a agirem de uma maneira desejada quanto para dissuadi-las de agir de uma maneira indesejada.

O livro resultou de extensa pesquisa realizada desde 2015. Foi escrito com um enfoque didático, traduzindo conceitos de ciberdefesa e cibersegurança para "não-iniciados" e oferecendo uma visão estratégica. Para tanto, reorganiza, atualiza e complementa informações e análises desenvolvidas no Doutorado em Ciências Militares no Instituto Meira Mattos, da Escola de Comando e Estado-Maior do Exército (ECEME) e no King's College London (Reino Unido) e no Mestrado em Estudos de Guerra no King's College, bem como em cerca de uma dezena de artigos publicados em revistas acadêmicas ou especializadas, e outras tantas participações em congressos e seminários.

Adota-se um enfoque particular voltado a nações com uma cultura não-agressiva, como é a tradição brasileira, concluindo-se que é possível desenvolver um Software Power nacional capaz de apresentar efeito dissuasório contra perpetradores de ciberofensas, e que o desenvolvimento de tais capacidades pode representar uma oportunidade estratégica para a desejada inserção internacional do Brasil.

1.1 Sobre a Terminologia Adotada

Diversos termos usados neste livro têm semântica própria, devendo ser entendidos em seu significado específico.

1.1.1 "Ciber"coisas

Adota-se neste livro o adjetivo "cibernética", em suas flexões de gênero e número – cibernética(s) ou cibernético(s) – substituído pelo prefixo *ciber* associado ao substantivo ao qual se refere, em conformidade com as regras do Novo Acordo Ortográfico da Língua Portuguesa. Este padrão, também utilizado pelo Secretário Geral da ONU António Guterres, é adotado em Portugal e nos documentos em língua portuguesa emitidos pela União Europeia, gerando termos como: ciberespaço, cibercrime, cibersegurança, ciberdefesa, ciberdissuasão, ciber-higiene e ciber-resiliência, dentre outros[1].

1.1.2 Autocontenção e Contenção

Optou-se pelo uso de autocontenção, ainda que o termo original em inglês *restraint* pudesse ser traduzido apenas como "contenção". No entanto, esta palavra também é utilizada em português para traduzir o termo *containment*, que tem outro significado relevante na Teoria da Dissuasão, também presente neste trabalho. Por essa razão neste trabalho utilizamos o termo autocontenção para o sentido de *restraint* e contenção para o sentido de *containment*.

1.1.3 Coação ou Coerção?

Embora em língua portuguesa as palavras "coerção" e "coação" sejam usualmente consideradas sinônimas, seus significados exatos denotam situações distintas: coerção representa "a força exercida pelo Estado para fazer valer o direito", o uso legal da força por autoridades para impor leis e obrigar ao seu cumprimento; coação representa o uso de

[1] Comissão Europeia, "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE - Comunicação Conjunta ao Parlamento Europeu e ao Conselho"; Parlamento Europeu, "RELATÓRIO sobre ciberdefesa (2018/2004(INI)) - A8-0189/2018".

"violência física ou moral imposta a alguém para que faça, deixe de fazer ou permita que se faça alguma coisa", levando-a a agir contra sua vontade ou impedi-la de agir conforme seu interesse[2].

Outrossim, o termo coação é mais adequado para traduzir o conceito proposto na *Coercion Theory* de Thomas Schelling[3].

1.1.4 Dissuasão x Deterrência

Em língua portuguesa não existe um termo específico para diferenciar os termos em língua inglesa *dissuasion* e *deterrence*, sendo comumente utilizada a palavra "dissuasão" em ambos os casos. Dada a relevância da diferenciação dos dois conceitos para o escopo deste trabalho, tomamos emprestado da Estratégia Nacional de Defesa (END) o neologismo "deterrência" usado aqui para o sentido de *deterrence*, enquanto usamos o clássico termo "dissuasão" para o sentido de *dissuasion*. Observa-se, no entanto, que a END considera deterrência e dissuasão como sinônimos[4], do que divergimos frontalmente, pelas razões expostas no Capítulo 4.

Em função da opção pelo uso do termo deterrência, foi preciso adaptarmos outros termos derivados:

- Deterrente: aquele ou aquilo que exerce deterrência;
- Deterrido: aquele que é objeto da deterrência;
- Deterrer: verbo que indica a ação de exercer a deterrência. Não cabe o uso do verbo "deter", que possui significado diverso.

---

[2] Houaiss e Villar, *Dicionário Houaiss da Língua Portuguesa*.

[3] Schelling, *Arms and influence: With a new preface and Afterword*.

[4] Brasil-MD, "Política Nacional de Defesa e Estratégia Nacional de Defesa", 76.

1.2 Introdução, Contexto e Motivação

Nos últimos anos, tornou-se senso comum considerar o ciberespaço como o quinto domínio da guerra, depois da terra, do mar, do ar e do espaço sideral. Neste quinto domínio, os Estados Unidos da América (EUA), como em todos os outros domínios, procuram preservar a sua supremacia, mantendo a vantagem conquistada com sua superioridade histórica no desenvolvimento dos computadores e da Internet, bem como na produção de software. Outras "ciberpotências", como o Reino Unido (UK, da sigla em inglês), França e Israel, também desenvolvem capacidades ofensivas avançadas. Países como China, Rússia, Coreia do Norte e Irã também utilizam amplamente o ciberespaço como um recurso de política internacional.

Ao mesmo tempo, *think tanks* norte-americanos debatem uma nova "grande estratégia" para os EUA, na qual é necessário decidir entre os limites da autocontenção (*restraint*) e da primazia (*primacy*)[5]. A tendência à autocontenção é evidente nos anúncios de retirada de tropas ou redução das forças militares norte-americanas da Europa e da Ásia, em particular do Oriente Médio. Esta autocontenção deveria servir para forçar os aliados europeus e asiáticos dos EUA a investirem mais em sua própria defesa e ajudar a aliviar os combalidos cofres norte-americanos. Ela também evita os "sacos pretos" (*body-bags*) que, televisionados, geram um enorme desgaste político. No entanto, nem a perspectiva da autocontenção nem aquela da primazia indicam que os EUA virão a reduzir sua presença ou agressividade no ciberespaço[6]. De fato, a opção por uma presença militar cinética (ou física) global mais limitada liberaria recursos para uma presença

[5] Mazarr, "The world has passed the old grand strategies by".

[6] Gompert e Binnendijk, "Time for Washington to amp up the power to coerce".

ainda mais agressiva no ciberespaço, como forma de compensação pela perda da presença global tradicional. Além disso, os vastos recursos liberados pela opção da autocontenção também poderiam ser aplicados pelos EUA no "hemisfério americano", com o objetivo de amplificar e assegurar seu domínio e influência nesta área.

Além disso, "ferramentas de software" há muito são utilizadas para espionagem, sabotagem, crime ou ativismo, patrocinados ou não por estados. Entre muitos exemplos, o caso Snowden, em particular, revelou uma grande operação de espionagem estatal. Envolvia espionagem política, relacionada às comunicações pessoais da Chanceler da Alemanha, dos Presidentes de Brasil e México, de alguns de seus ministros, além de milhares de outras pessoas. Fora do âmbito político, Snowden também denunciou a espionagem sistemática da Petrobras, a estatal brasileira de petróleo que havia anunciado a descoberta de gigantescas reservas de petróleo em águas jurisdicionais brasileiras alguns anos antes.

Espionagem, sabotagem, crime e ativismo, em geral, são temas relacionados à segurança e, por si só, justificariam as nações investirem em seu Software Power. No entanto, antes do Caso Snowden, houve um caso notavelmente diferente, denominado Stuxnet. Embora influentes estudiosos de ciberconflitos como Thomas Rid[7] discordem, pela primeira vez (conhecida) um software foi usado por um estado-nação para impor sua vontade política a outro, usando de violência, na forma de destruição física de máquinas, e mesmo letalidade, na ótica do ataque a um *interesse vital* de uma nação soberana. Sabe-se que "um ato de força para **compelir nosso inimigo a fazer nossa vontade**" é um ato de guerra[8]. Nos termos de

[7] Rid, *Cyber War Will Not Take Place*.

[8] Clausewitz, *On War*, 75, tradução livre, grifo nosso.

Thomas Schelling[9], um exemplo claro de compelimento, no qual um ator racional é levado a decidir contra sua vontade. Stuxnet, portanto, foi um "divisor de águas" quando introduziu uma razão ainda mais fundamental para as nações buscarem desenvolver seu Software Power: defesa!

Num exemplo mais contemporâneo, a comunidade de inteligência norte-americana atribuiu à Rússia os ataques ao Partido Democrata e o vazamento seletivo de informações contrárias ao candidato democrata e favoráveis ao candidato republicano, o qual viria a se sagrar vencedor do pleito, indicando que os russos tentavam influenciar as eleições presidenciais norte-americanas de 2016[10]. Na semana seguinte, o Presidente dos EUA Barack Obama declarou que a Casa Branca estudaria respostas proporcionais, enquanto o chanceler russo Sergei Lavrov disse à CNN que a Rússia "não nega", mas "não vimos um único fato, uma única prova"; "se eles decidirem fazer algo, deixe-os fazer", disse ele[11].

Embora os EUA sempre se queixem das ofensas promovidas por chineses, russos, norte-coreanos e iranianos ao seu ciberespaço, existe uma corrente crítica que coloca os próprios norte-americanos no polo mais agressivo deste espaço[12]. Conceitualmente, o mesmo poder cibernético que os americanos teriam usado contra o Irã está agora sendo usado contra eles pelos russos, essencialmente com o mesmo propósito: coação por compelimento.

---

[9] Schelling, *Arms and influence: With a new preface and Afterword*.

[10] Paletta, "U.S. Blames Russia for recent hacks".

[11] Krever e Smith-Spark, "Lavrov denies Russian influence over US election".

[12] Austin, "Sino-US tensions in Cyberspace: All China's fault?"; Harris, *@War: The rise of the Military-Internet complex*.

Schelling[13] determinou que, além das capacidades, a credibilidade era um elemento essencial de dissuasão por ameaça de punição (ou pelo medo), associada principalmente à "determinação" ou "vontade" (*will*) de se empregar os meios de retaliação disponíveis. Essa determinação estaria relacionada à "personalidade" ou "cara" (*face*) de um país: sua reputação para a ação, a expectativa que outros países têm sobre seu comportamento. Após a Segunda Guerra Mundial, entre os integrantes do G-20, apenas Brasil, Alemanha, México e Japão não se envolveram em ações agressivas, conforme definição da Organização das Nações Unidas (ONU), exceto em operações sancionadas pela própria ONU ou por entidades multilaterais regionais onde todos os envolvidos eram membros. Esses quatro países, portanto, têm uma "cara" de nações não-agressivas. Mesmo assim, todos foram espionados pela Agência de Segurança Nacional dos EUA (NSA) e outros membros do grupo Five-Eyes (comunidades de inteligência dos EUA, Reino Unido, Canadá, Austrália e Nova Zelândia)[14]. Além disso, eles também são espionados pela China e pela Rússia, e possivelmente por outros[15].

Nesse contexto geopolítico, e considerando o desejo e a necessidade de inserção internacional do Brasil, um "olhar brasileiro" sobre o ciberpoder dos estados-nação e sua utilização como instrumento de coação no cenário internacional torna-se relevante para o entendimento de como esse ciberpoder pode afetar a soberania nacional. De fato, os casos recentes de ciberofensas tornados públicos internacionalmente demonstram que o Brasil precisa estar

---

[13] Schelling, *The Strategy of Conflict*.

[14] Greenwald, *No place to hide: Edward Snowden, the NSA and the surveillance state*.

[15] Wagstyl, "Germany points finger at Kremlin for cyber attack on the Bundestag".

preparado para evitar se tornar uma presa fácil para nações interessadas no uso desses instrumentos. O caso Snowden, em particular, mostrou que os norte-americanos realizaram operações de espionagem política e econômica que afetaram o país[16]. Antes, embora não visasse atacar o Brasil em particular, o malware Stuxnet também infectou infraestruturas críticas brasileiras que utilizavam sistemas de controle industrial fornecidos pela empresa alemã Siemens[17]. Fosse o Brasil o alvo pretendido, sem dúvida o país teria sofrido efeitos nocivos e potencialmente catastróficos.

1.3 O Cerne do Problema

O núcleo do livro consiste em demonstrar o que é o Software Power ("Poder de Software") e como ele pode ser usado como uma ferramenta de coação interestatal, no sentido de estados-nação dissuadirem seus pares de adotarem ações indesejadas ou de compeli-los a praticarem ações desejadas, notadamente no tocante a ciberofensas patrocinadas por estados.

Em particular, considerando que a corrente principal da literatura disponível sobre ciberdissuasão (e ciberdeterrência), principalmente de países membros da OTAN, indica que a ciberdissuasão por medo (ou por ameaça de punição), com capacidades de retaliação não necessariamente "de mesma natureza" ou "na mesma moeda" (*in kind*), é a única alternativa economicamente viável para a dissuasão de ciberofensas, visto que a dissuasão por negação seria muito cara e que um "perímetro seguro" não se mostra viável em termos cibernéticos[18].

---

[16] Greenwald, *No place to hide: Edward Snowden, the NSA and the surveillance state*.

[17] Falliere, Murchu, e Chien, "W32.Stuxnet Dossier".

[18] Nye, "International Norms in Cyberspace".

Embora se busque "um olhar brasileiro" sobre o tema, tanto o referencial teórico quanto os dados empíricos coletados indicam a possibilidade concreta de uso de raciocínio indutivo para concluir pela aplicabilidade das premissas a um conjunto mais amplo de países.

Ademais, as fontes utilizadas foram exclusivamente fontes abertas: documentos oficiais de várias nações e agências multilaterais, livros, relatórios, artigos acadêmicos e de notícias, vídeos, palestras e notas de conferências, em particular da Escola Superior de Guerra (ESG), do King's College London (KCL) e da Escola de Comando e Estado-Maior do Exército (ECEME), aulas de mestrado e doutorado, seminários e debates, bem como de congressos e workshops no Brasil e no exterior. Além disso, visitas técnicas e conversas com o pessoal do Comando de Defesa Cibernética (ComDCiber) do Brasil forneceram valiosas informações não sigilosas.

1.4 Estrutura do Livro

O livro foi estruturado para, de forma didática e elucidativa, sistematizar os conceitos e "jogar uma luz" sobre as características e potencialidades do uso militar do ciberespaço. Para tanto, o Capítulo 2 o conceito de Software Power (Poder de Software) e os motivos para enfatizá-lo em contraposição ao Hardware Power (Poder de hardware). O Capítulo 3 descreve a natureza e as características das "Ciberofensas Praticadas por Estados", considerando suas motivações, tipos de operações e as características dos "ciberguerreiros". O Capítulo 4 dedica-se às "Ciberarmas" e suas particularidades comparadas às armas convencionais. O Capítulo 5 descreve o que seria "Ciberdissuasão", enquanto instrumento para evitar a cibercoação e sua potencial escalada para outros tipos de conflitos. Em seguida, o Capítulo 6 descreve "Os Seis Tipos de Ciberdissuasão" adaptando aos ciberconflitos as características dos seis tipos de dissuasão

identificados em outro livro de nossa série, “Dissuasão: Um Olhar Brasileiro”.

Por fim, à guisa de “Conclusão”, o Capítulo 7 faz um apanhado dos temas abordados nos capítulos anteriores, consolidando as ideias apresentadas e as conclusões da pesquisa, apontando seus pontos fortes e fracos, e possíveis desenvolvimentos futuros.

2 Poder de Software (*Software Power*)

Este capítulo explica o conceito de "Poder de Software" (*Software Power*), partindo da noção de ciberpoder (*cyber power*) como tendo duas partes constitutivas: Poder de Hardware (*Hardware Power*) e Poder de Software (*Software Power*).

2.1 Introdução

Uma definição comumente aceita de ciberpoder afirma que ele é "a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e por meio dos instrumentos de poder"[1].

Nye[2] definiu *Soft Power* ("Poder Brando") como a capacidade de atrair e persuadir, enquanto o *Hard Power* ("Poder Duro") seria a capacidade de coagir. Embora aqui "brinquemos" com a terminologia original de Nye, é essencial esclarecer que tanto o *Hardware Power* quanto o *Software Power*, conforme definidos no contexto deste trabalho, são exemplos de "Poder Duro" em seu conceito original.

Os conceitos de ciberpoder, *soft power* e *hard power* mencionados anteriormente lidam com muitos dos elementos que constituem a base da Teoria da Influência: influência, persuasão e coação. Estes, e seu uso no ciberespaço, constituem uma parte essencial deste livro.

---

[1] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem".

[2] Nye, *Soft Power: The Means To Success In World Politics*.

2.2 Ciberpoder

"Pode um exército de magos de software usar meios eletrônicos traiçoeiros para deslocar os sistemas de apoio das sociedades modernas, como transporte, bancos e saúde pública?"[3]. Esta questão apresenta os dois elementos centrais do chamado ciberpoder: o software, cujos "feiticeiros" usariam "meios eletrônicos insidiosos", o hardware, para atingir seus objetivos.

O ser humano tem uma percepção clara da materialidade das coisas. A mesma clareza existe em relação aos artefatos militares cinéticos da era industrial: aeronaves, veículos blindados, mísseis e divisões de exércitos. Eles são historicamente valorizados como símbolos de poder. Em maio de 1935, o chanceler francês Laval entrevistou Stalin para discutir um pacto entre a França e a União Soviética (URSS). Depois de três dias debatendo a força do exército francês, Laval perguntou se Stalin poderia encorajar a religião e os católicos na Rússia, argumentando que isso poderia ajudar junto ao Papa. Stalin respondeu: "Oh! O Papa! Quantas divisões ele tem?" [4]. Em termos cibernéticos, a pergunta de Stalin corresponderia a algo como "quantos supercomputadores ele tem?". A materialidade corresponde ao hardware.

É muito mais difícil de se perceber a importância do conhecimento, o combustível da era pós-industrial, que é imaterial, abstrato: sem forma, sem cor, sem peso, sem cheiro; os sentidos humanos não podem percebê-lo. Em termos cibernéticos, é chamado de software.

---

[3] Freedman, *Strategy: A history*, 228, tradução livre.

[4] Churchill, *The Second World War, Volume 1: The Gathering Storm*, 121, tradução livre.

Existem alguns argumentos convincentes para considerar o ciberpoder em sua totalidade (hardware + software). Por exemplo, hardware e software dependem um do outro; ataques de um lado podem afetar o outro [5]. Além disso, o Exército dos EUA trabalha com o conceito de Atividades Eletromagnéticas Cibernéticas (CEMA), definido "como um esforço unificado onde as operações de ciberguerra e guerra eletrônica devam ser integradas e sincronizadas, percebidas como um ambiente operacional único" [6]. No entanto, as nações em desenvolvimento têm dificuldades para o desenvolvimento de hardware. Assim, o software torna-se mais viável para elas. O Brasil, por exemplo, é deficiente "principalmente na camada de hardware, devido ao histórico de baixos investimentos em ciência e tecnologia", enquanto, em software, "o país desempenha importante papel e vem se posicionando como um dos maiores produtores de programas do mundo"[7]. Mais argumentos que apoiam o foco no Software Power, principalmente quando os recursos para desenvolvimento de hardware são limitados, são discutidos em maior profundidade mais adiante.

O termo poder cibernético, "parte de uma linhagem terminológica que inclui 'poder aéreo' e 'poder marítimo' para descrever as operações do poder coativo nacional, principalmente militar, em domínios ambientais particulares" carece de definições claras e precisas[8].

---

[5] Gama Neto e Lopes, "Armas Cibernéticas e Segurança Nacional".

[6] Gama Neto, "Guerra cibernética/Guerra eletrônica – conceitos, desafios e espaços de interação".

[7] Guedes de Oliveira e Portela, "As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil", 77.

[8] Betz e Stevens, *Cyberspace and the state: Towards a strategy for Cyberpower*, 43.

Para evitar tal imprecisão, o termo "Software Power" foi concebido para designar:

> Ferramentas de software usadas em nome de um estado para explorar, negar, degradar, interromper, destruir ou defender redes de computadores, seus dispositivos conectados e sistemas de informação ou dados neles residentes[9].

Em termos práticos, recursos de software ofensivos e defensivos relacionados a ciberoperações originadas por estados visando outros estados.

Esta definição reúne os três subconjuntos de Operações de Redes de Computadores (CNO): Exploração de Redes de Computadores (CNE), Ataque a Redes de Computadores (CNA) e Defesa de Redes de Computadores (CND)[10]. Ela também estende esses conceitos para incluir não apenas "redes de computadores", mas também todos os dispositivos a elas conectados, bem como sistemas e dados que nelas residem[11]. Por fim, especifica o software utilizado em ciberoperações "em nome de um estado", incluindo a já clássica definição de Libicki[12].

A definição dada também exclui PsyOps (operações psicológicas) e operações de influência, por vezes chamadas de Guerra Informacional ou Guerra Híbrida, que consistem no uso de redes sociais, como Twitter ou Facebook, para a desestabilização de governos, como ocorreu durante a Primavera Árabe, ou para influenciar eleitores em pleitos nos EUA e em diferentes países da Europa ocidental. Também

---

[9] Malagutti, "Software Power".

[10] Klimburg e Tirmaa-Klaar, "Cybersecurity and Cyberpower : Concepts , Conditions and Capabilities for Action Wihtin the EU", 7.

[11] Malagutti, "Software Power".

[12] Libicki, "Cyberdeterrence and Cyberwar", 23.

evita discussões infrutíferas sobre a cibernética apresentar "áreas de sombreamento" no tocante à guerra eletrônica. De acordo com a definição utilizada neste trabalho, explorar uma vulnerabilidade de rede por meio de software, ou "hackear" remotamente um veículo aéreo não tripulado (*drone*) é uma operação de "Software Power". Utilizar sinais de rádio para interferir na capacidade de comunicação e controle desse mesmo *drone* não constitui este tipo de operação. A definição acima também exclui operações não patrocinadas por estados, motivadas ou não por intenções políticas[13].

2.3 "Poder de Hardware" Não É Irrelevante

O foco no "Software Power" não pretende indicar que o "Hardware Power" seja irrelevante.

> Qual país possui o computador mais rápido do mundo importa tanto para os formuladores de políticas agora quanto qual país possuía a aeronave mais rápida ou de maior alcance no período entre guerras e pela mesma razão. Eles são considerados indicativos de potencial militar, bem como de prestígio.[14]

A unidade utilizada para se medir o poder computacional dos supercomputadores atuais é denominada PFLOPS (PetaFLOPS), que significa 1.000^5 (mil elevado à quinta potência), o que resulta no prefixo grego "peta", uma escala de 5, associado ao nome desta unidade, correspondendo a 10^{15} operações de ponto flutuante por segundo.

A Tabela 2-1 mostra os cinco mais potentes supercomputadores do mundo em novembro de 2015.

Tabela 2-1 - Maiores supercomputadores em novembro de 2015.

---

[13] Malagutti, "Software Power".

[14] Betz e Stevens, *Cyberspace and the state: Towards a strategy for Cyberpower*, 86.

Posição	País	Computador	PFLOPS
1	China	Tianhe-2	33,9
2	EUA	Titan	17,6
3	EUA	Sequoia	17,2
4	Japão	RIKEN	10,5
5	EUA	Mira	8,6

Fonte: Compilado pelo autor com dados de TOP500.org[15].

Na atualização posterior da lista, em junho de 2016, um novo computador chinês, o Sunway TaihuLight, ocupou a primeira posição, com 93,0 PFLOPS de capacidade, quase três vezes mais rápido que seu conacional Tianhe-2 e cinco vezes mais rápido que o Titan norte-americano[16].

A despeito do enorme poder de processamento do TaihuLight, ele foi baseado em um processador de 256 núcleos projetado e construído na China[17]. No entanto, enquanto os chineses podem (e devem) se orgulhar de sua dupla conquista, os norte-americanos também ampliaram suas capacidades. Naquele mesmo junho de 2016, uma universidade norte-americana anunciou a criação do primeiro processador kilo-core (1024-núcleos), quatro vezes mais núcleos que o recém-lançado processador chinês[18].

Foi apenas em junho de 2018 que os norte-americanos destronaram o TaihuLight, com o Summit. Ele tinha um quarto dos núcleos de seu concorrente chinês (“apenas” 2.282.544 núcleos contra os 10.649.600 do oponente) e alcançou impressionantes 122,3 PFLOPS de capacidade sustentada. Os EUA também apresentaram um novo

[15] TOP500.org, “Top500 November 2015”.

[16] TOP500.org, “Top500 June 2016”.

[17] Fu et al., “The Sunway TaihuLight supercomputer: system and applications”.

[18] Fell e Bass, “World ’ s First 1,000-Processor Chip”.

supercomputador que assumiu a terceira posição no ranking, o Sierra, com 71,6 PFLOPS de capacidade sustentada[19].

A lista não mudou muito até junho de 2020 (refletida na Tabela 2-2), quando o computador japonês Fugaku "furou a fila" e alcançou o primeiro lugar, com mais de três vezes o poder computacional do Summit, posição mantida até hoje. De fato, uma das mudanças observadas foi um ligeiro aumento na capacidade sustentada do Fugaku na lista mais recente[20].

Tabela 2-2– Maiores supercomputadores em novembro de 2021.

Posição	País	Computador	PFLOPS
1	Japão	Fugaku	442,0
2	EUA	Summit	148,6
3	EUA	Sierra	94,6
4	China	TaihuLight	93,0
5	EUA	Perlmutter	70,9
6	EUA	Selene	63,5
7	China	Tianhe-2	61,4

Fonte: Compilada pelo autor com dados do TOP500.org[21].

Capacidades de processamento superiores são essenciais para tarefas de importância militar e econômica, como criptoanálise ou simulação precisa de reações nucleares ou reações químicas em nível molecular.

Em 2017, a União Europeia (UE) listou algumas preocupações relativas à pequena participação europeia no

[19] TOP500.org, "Top500 June 2018".

[20] TOP500.org, "TOP500 November 2021".

[21] TOP500.org.

mercado internacional de supercomputadores, ou computação de alto desempenho (HPC, do acrônimo em inglês)[22]:

1) A ausência de supercomputadores de nações da União Europeia na lista dos 10 maiores supercomputadores;
2) A necessidade de maior poder computacional para pesquisas avançadas;
3) O fato de os europeus participarem com 5% dos recursos mundiais de supercomputação, embora consumindo um terço dessa capacidade computacional;
4) A inexistência de uma cadeia de suprimento na indústria europeia capaz de abastecer o mercado de forma competitiva em relação aos EUA, China e Japão;
5) O risco de ficar tecnologicamente desprovido ou ficar para trás em *know-how* para inovação e competitividade;
6) O risco de ter dados produzidos por pesquisadores e indústrias da UE processados em outros lugares por falta de capacidades correspondentes na Europa.

Essa preocupação levou a União Europeia a iniciar o projeto EuroHPC (*European High-Performance Computing Joint Undertaking*), cujo objetivo central é fomentar os investimentos europeus no segmento de supercomputação. Parte desse fomento consistiu na injeção de aproximadamente um bilhão de euros no período 2018-2020[23].

---

[22] European Comission, “High Performance Computing (HPC) Factsheet”.

[23] European Comission, “High-Performance Computing”.

Noutra seara, expandir as atuais capacidades de processamento de alto desempenho é uma das promessas da pesquisa em computação quântica[24]. Em 2020 o governo dos EUA anunciou um novo plano de financiamento de cinco anos para centros de pesquisa em computação quântica: US$ 625 milhões do Departamento de Energia e US$ 300 milhões dos próprios centros de pesquisa[25].

Para mensurar o salto quantitativo esperado na capacidade de processamento, estima-se que, já em 2022, se passe de "petascale" para "exascale" (1.000^6 FLOPS), correspondendo a mil PFLOPS, ou 10^{18} FLOPS. De fato, o supercomputador japonês Fugaku, embora não baseado em tecnologia quântica, já alcançou 0,41 EFLOPS (ExaFLOPS) de capacidade computacional.

2.4 Por Que Focar no Poder de Software?

Apesar da importância do hardware, a ênfase no Software Power observada neste trabalho se deve a diferentes razões objetivas.

2.4.1 Todo Malware É Software!

Até o momento, todas as ciberofensas relevantes tornadas públicas estão relacionadas a vulnerabilidades de recursos de software, e não às de hardware. Em geral, os ciberataques consistem na transmissão de software ou dados

[24] The Economist, "After Moore's Law"; Financial Times, "Quantum computing rivals muster software power in new ' arms race '"; Biercuk e Fontaine, "The Leap into Quantum Technology: A Primer for National Security Professionals"; Owen e Gorwa, "Quantum Leap: China's Satellite and the New Arms Race".

[25] US-White House, "The Trump Administration Is Investing $1 Billion in Research Institutes to Advance Industries of the Future | The White House".

espúrios para uma rede alvo com o intuito de explorar vulnerabilidades ou danificar a própria rede ou os sistemas ou dados nela contidos[26].

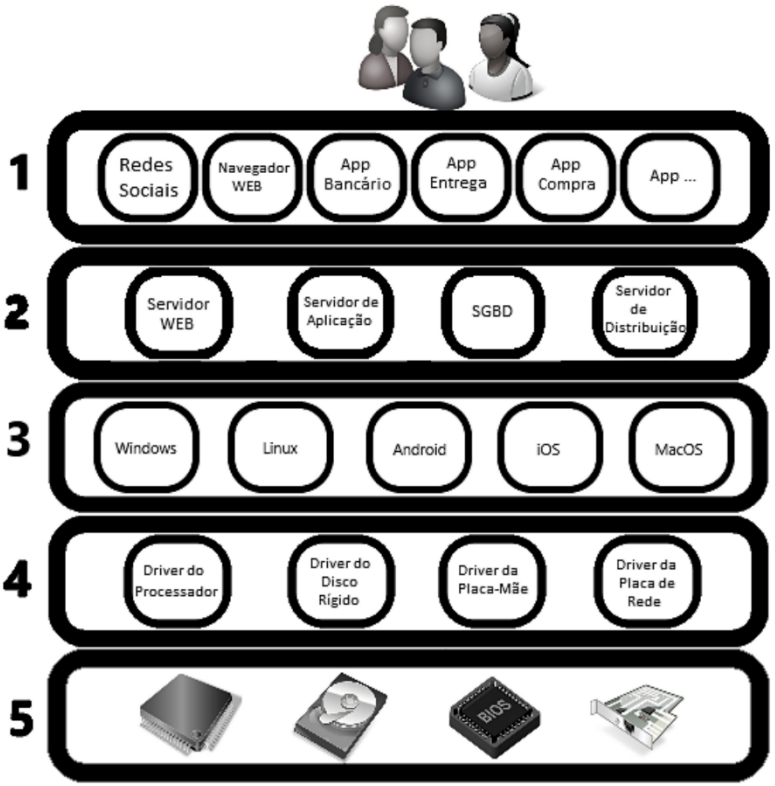
2.4.2 Software É o Que "Dá Vida" ao Hardware!

Conforme explicitado na pergunta apresentada no início deste capítulo, é a "mágica" do software que controla o hardware. Isso ocorre em diferentes níveis.

O software está presente em muitas "camadas" em qualquer dispositivo de computação moderno. A Figura 2-1 representa as diferentes camadas de uma forma bastante simplificada, buscando ser o mais didática possível.

Figura 2-1 – Camadas de Software

[26] Lukasik, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains".



Fonte: Compilada pelo autor.

Na camada 1, aquela mais próxima ao usuário, temos o contexto dos aplicativos (ou *Apps*) que realizam as tarefas finalísticas do usuário, processando os dados, apresentando informações para suporte a decisão ou controlando o fluxo dos processos de negócios.

A camada 2 contém aquilo que se denomina *middleware*, software intermediário que suporta as aplicações. Pode-se exemplificar com o servidor web Apache Tomcat, os servidores de aplicação JBoss e .NET Framework, ou gerenciadores de banco de dados mySQL ou

Oracle, bem como as plataformas de processamento distribuído (ou servidores de distribuição) Hadoop, Accumulo, BOINC ou FAH, discutidas mais adiante.

A terceira camada representa o contexto dos Sistemas Operacionais (SOs), exemplificados por Windows, Linux, Android, macOS ou iOS, os cinco mais populares do mercado. SOs são softwares que gerenciam recursos de hardware, como memória, processadores e outros dispositivos, alocando-os aos aplicativos (camada 1) ou ao *middleware* (camada 2) conforme as demandas destes e a disponibilidade do equipamento.

A quarta camada de software é normalmente invisível à maioria dos usuários, e consiste naquele dos "direcionadores" (*drivers*) que conectam os Sistemas Operacionais (camada 3) aos respectivos dispositivos de hardware, como processador central (CPU), placa-mãe, placa de vídeo (GPU), placa de rede, Blue Tooth, WiFi, teclado, mouse, impressoras ou ainda as chamadas *Programmable Logic Controllers* (PLCs), dispositivos que desempenham funções de controle e monitoramento de máquinas e processos industriais complexos, como aqueles das centrífugas de enriquecimento de urânio na usina nuclear iraniana de Natanz, alvo do Stuxnet.

A quinta e última camada, aquela mais "baixa", é a do *firmware* (microcódigo) executado nos próprios componentes das placas de circuito eletrônico, que interagem com os "direcionadores" (camada 4), a exemplo do BIOS dos computadores pessoais.

Cada uma dessas camadas representa uma "superfície de ataque" (ou "vetor de ataque") passível de exploração, com vulnerabilidades particulares que podem levar a diferentes complexidades de proteção e ataque, bem como de efeitos.

2.4.3 Software Pode Ser Operado Remotamente

Embora o "hardware possa ser desligado ou destruído, deliberada ou acidentalmente", isso requer uma presença física no local, enquanto, remotamente, "software pode ser alterado, permitindo ações que antes eram impedidas ou vice-versa"[27].

Nem mesmo sistemas "*air gapped*", apartados ou desconectados de redes externas, ficam imunes. As centrífugas iranianas de Natanz ficavam numa rede apartada, mas a partir do momento em que um computador dessa rede foi contaminado, o Stuxnet chegou ao controle das centrífugas e iniciou seu processo de ataque[28].

2.4.4 Software Pode Substituir Hardware

No processo de evolução tecnológica, de forma similar àquela como a eletrônica substituiu a mecânica em uma ampla gama de usos, o software vem substituindo o hardware. Algoritmos de computação paralela implementados por software tornaram computadores comerciais comuns de baixo custo, interconectados em *clusters*, capazes de processar grandes volumes de dados em velocidades nunca imaginadas. A agência britânica de inteligência de sinais GCHQ, por exemplo, usa a plataforma de software de código aberto Hadoop, inspirada no MapReduce do Google, para analisar metadados de comunicações eletrônicas[29]. Esta plataforma foi projetada para fornecer "processamento distribuído de grandes

---

[27] Stevens e Betz, "Analogical Reasoning and Cyber Security", 152.

[28] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*.

[29] Dean e Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters"; UK-GCHQ, *HIMR Data Mining Research Problem Book*.

conjuntos de dados em *clusters* de computadores usando modelos de programação simples"[30]. "Com centenas de discos rígidos trabalhando simultaneamente, vários gigabytes podem ser lidos por segundo. Isso permite o processamento dos conjuntos de dados de vários terabytes que interceptamos"[31]. Em 2008, a homóloga norte-americana do GCHQ, a National Security Agency (NSA), desenvolveu a plataforma Accumulo, também baseada na tecnologia Google[32]. Posteriormente, em 2011, a NSA disponibilizou a plataforma Accumulo como *open-source*[33].

Enquanto as plataformas acima são capazes de lidar com grandes volumes de dados para necessidades de processamento relativamente simples, o experimento SETI@home (*Search for Extraterrestrial Intelligence at Home*), gerenciado pela Universidade de Berkeley, produziu o Berkeley Open Infrastructure for Network Computing (BOINC), plataforma de computação distribuída cooperativa voluntária. "Voluntária" pelo fato de que um usuário de computador instala voluntariamente um software que "compartilha" o poder computacional disponível de seu equipamento. Exemplificando, quando um computador pessoal entra no modo "proteção de tela", seu processador começa a executar tarefas de processamento distribuído para um dos projetos usando o aplicativo da plataforma BOINC. Em 27 de agosto de 2020, a plataforma registrou uma média de 859.385 computadores ativos, gerando 26,0 PFLOPS[34].

---

[30] Apache Software Foundation, "Apache Hadoop".

[31] UK-GCHQ, *HIMR Data Mining Research Problem Book*, 60.

[32] Metz, "NSA mimics Google, Pisses off senate"; Harris, *@War: The rise of the Military-Internet complex*, 36.

[33] Apache Software Foundation, "Apache Accumulo".

[34] BOINC, "BOINC".

Esse poder de computação o colocava como o 8º "supercomputador" mais potente do mundo.

Outra plataforma de computação distribuída voluntária é a Folding@home (ou FAH), usada para computar o "dobramento de proteínas" em busca da cura para doenças como o câncer, a esclerose lateral amiotrófica e, desde janeiro de 2020, a Covid-19. Além de usar o poder de processamento regular das CPUs, ela também usa os recursos superiores das Unidades de Processamento Gráfico (GPUs) e consoles de jogos [35]. Em agosto de 2020, a página de estatísticas desta plataforma havia reportado, em 50 dias, os dados de desempenho apresentados na Tabela 2-3.

Conforme relatado, os 16,7 milhões de núcleos associados voluntariamente foram capazes de fornecer 1.169,3 PFLOPS (ou 1,17 EFLOPS), quase três vezes o poder de computação do poderoso hardware do Fugaku.

Tabela 2-3 – Poder computacional da plataforma Folding@home.

SO	AMD GPUs	Nvidia GPUs	CPUs	Núcleos	PFLOPS
Linux	8.024	436.173	1.842.044	14.877.878	943,1
Windows	27.480	98.162	263.218	1.666.878	224,5
macOSX	10	0	36.787	153.748	1,7
Total	***35.514***	***534.335***	***2.142.049***	***16.698.504***	***1.169,3***

Fonte: Compilado pelo autor com dados do Folding@home[36].

Em outras palavras, o primeiro computador exascale apareceu já em 2020 (não em 2022, como esperado), e foi provido por software, e não por hardware quântico.

---

[35] Folding@home, "Front Page - Folding@home".

[36] Folding@home, "Folding@home stats report".

2.4.5 Ciberpotências Prescindem de Supercomputadores

A disponibilidade de poder de hardware expressivo não é significativa em vários dos países que figuram como superpotências cibernéticas ou os que constituem as maiores economias mundiais, como mostra a Tabela 2-4.

Tabela 2-4 –Maiores supercomputadores dos demais países do G-20.

Posição	País	Computador	PFLOPS
8	Alemanha	JUWELS	44,1
9	Itália	HPC-5	35,5
11	Coreia do Sul	SSC-21	25,2
14	França	CEA-HF	23,2
15	Arábia Saudita	Damman-7	22,4
19	Rússia	Chervonenkis	21,5
22	Reino Unido	Archer2	19,6
53	Austrália	Gadi	9,3
55	Brasil	Dragão	9,0
83	Canadá	Narval	5,9
102	Índia	Siddhi-AI	4,6
---	África do Sul	---	---
---	Argentina	---	---
---	Indonésia	---	---
---	México	---	---
---	Turquia	---	---

Fonte: Compilada pelo autor com dados do TOP500.org [37].

Como se observa, o maior supercomputador francês ocupa a 14ª posição, enquanto o mais potente

[37] TOP500.org, “TOP500 November 2021”.

supercomputador russo ocupa a 19ª colocação e o maior do Reino Unido figura apenas na 22ª. Israel não tem um único supercomputador listado entre os 500 maiores. Nem a Coreia do Norte ou o Irã. Assim, o poder do hardware não é determinante para se alcançar o status ciberpotência.

Poder-se-ia questionar que o maior computador de um país, isoladamente, não diz muito sobre o poder computacional total daquele país. Tomando-se isso em consideração, a Tabela 2-5 apresenta o poder computacional de todos os países representados na lista dos 500 maiores supercomputadores do mundo em novembro de 2021.

A capacidade computacional consolidada dos supercomputadores dos EUA soma quase 1 EFLOPS (986,5 PFLOPS) distribuídos em seus 149 sítios (quase 30% dos 500 sítios considerados). A do Japão é de 628,2 PFLOPS (dos quais 442 apenas no Fugaku) em seus 32 sítios computacionais (apenas 6,4% dos 500 sítios). A China tem 530,1 PFLOPS em seus 173 sítios (ou 34,5% dos 500 sítios). Por fim, vê-se também que, do quarto país, a Alemanha, em diante, a escala de poder computacional passa a ser outra, consideravelmente menor.

Os dados agregados confirmam que o Poder de Hardware não é determinante para alcançar o status de cibersuperpotência.

Tabela 2-5 – Maiores capacidades computacionais totais dentre os países com os 500 maiores supercomputadores em novembro de 2021.

País	#	PFLOPS	Sítios
EUA	1	986,5	149
Japão	2	628,2	32
China	3	530,1	173
Alemanha	4	181,4	26
França	5	117,0	19
Coreia do Sul	6	82,2	7
Itália	7	78,5	6
Rússia	8	73,7	7
Arábia Saudita	9	55,3	6
Reino Unido	10	54,9	11
Holanda	11	35,9	11
Canadá	12	29,6	11
Suíça	13	26,2	3
Brasil	14	22,0	5
Finlândia	15	13,4	3
Austrália	16	13,0	3
Luxemburgo	17	12,8	2
Suécia	18	12,3	4
Taiwan	19	11,3	2
Índia	20	11,0	3
República Tcheca	21	9,6	2
Polônia	22	9,3	4
Emirados Árabes Unidos	23	9,0	2

País	#	PFLOPS	Sítios
Eslovênia	25	6,9	2
Espanha	25	6,5	1
Noruega	26	4,7	1
Marrocos	27	3,2	1
Singapura	28	3,1	1
Áustria	29	2,7	1
Irlanda	30	2,0	1

Fonte: Compilada pelo autor com dados do TOP500.org[38].

2.4.6 Hardware Tem Uma "Barreira de Entrada" Alta

"Barreiras de Entrada" são características de um mercado ou segmento que o tornam difícil de ser ocupado por "novos entrantes" (novos competidores). Capacidades superiores de hardware apresentam uma alta barreira de entrada, devido não apenas ao custo de projeto de componentes eletrônicos, mas também ao de suas plantas de produção (fábricas e equipamentos) e ao fato de seu mercado ser muito limitado, ainda que de alto valor agregado.

2.4.7 Hardware Enfrenta Restrições de Exportação

A importação de supercomputadores é uma tarefa complexa, pois eles usualmente estão sob restrições de controle de armas (ou de produtos controlados ou sensíveis) por seus exportadores. O Brasil, por exemplo, sempre teve dificuldade em importar computadores e outros "materiais

[38] TOP500.org.

sensíveis", ou mesmo em adquirir equipamentos fabricados no Brasil por empresas norte-americanas[39].

As restrições não são aplicadas apenas a computadores prontos, mas também a seus componentes. O supercomputador chinês Tianhe-2, hoje o sétimo supercomputador mais poderoso do mundo, usa processadores da Intel, uma empresa norte-americana. Em meados de 2015, devido ao suposto uso daquele computador para simulação de reações nucleares, agências governamentais norte-americanas decretaram a restrição das exportações desses processadores para a China[40]. A resposta chinesa, obviamente planejada com antecedência, foi o lançamento do TaihuLight, já em 2016, construído exclusivamente com processadores chineses, como já mencionado anteriormente.

A despeito da enorme conquista chinesa, a diferença tecnológica dos processadores se reflete nos números da Tabela 2-6.

Tabela 2-6 – Consumo de energia dos maiores supercomputadores (em novembro de 2020).

#	País	Computador	PFLOPS	Núcleos	Potência (MW)	PFLOPS Por kCore	PFLOPS por MW
1	Japão	Fugaku	442,0	7.630.848	29,9	0,058	14,8
2	EUA	Summit	148,6	2.414.592	10,1	0,062	14,7
3	EUA	Sierra	94,6	1.572.480	7,4	0,060	12,8
4	China	TaihuLight	93,0	10.649.600	15,4	0,009	6,0

[39] Angelo, "'Eixo do mal' científico: Ministério pede explicações à Dell sobre exigências a físicos".

[40] Clark, "U.S. Agencies block technology exports for supercomputer in China".

#	País	Computador	PFLOPS	Núcleos	Potência (MW)	PFLOPS Por kCore	PFLOPS por MW
5	EUA	Selene	63,5	555.520	2,7	0,114	23,5
6	China	Tianhe-2	61,4	4.981.760	18,5	0,012	3,3

Fonte: Compilada pelo autor com dados do TOP500.org [41].

A coluna "PFLOPS por kCore" mostra quantos PFLOPS são gerados por grupo de 1.024 núcleos (um kCore), enquanto "PFLOPS por MW" indica o número de PFLOPS gerados por cada megawatt de energia consumida. Embora a capacidade nominal de PFLOPs do TaihuLight (China) não seja significativamente inferior à do Sierra (EUA), sua taxa de PFLOPs por kCore corresponde a apenas 15% daquela do computador norte-americano, e sua taxa de PFLOPs por MW corresponde a 47% da de seu concorrente. A diferença nesse último quesito é ainda maior quando se compara o TaihuLight com o Fugaku (Japão) e o Summit (EUA).

Depois que a Huawei decidiu não mais usar componentes de fabricantes norte-americanos, em 2019, a gigante chinesa começou a trabalhar para substituir esses componentes por versões nacionais[42]. Não obstante, mesmo essa estratégia ficou ameaçada quando o Departamento de Comércio dos EUA intensificou suas restrições em maio de 2020 e proibiu fabricantes de componentes de todo o mundo, que usem tecnologia dos EUA, de vender produtos para a Huawei[43]. Essa nova dificuldade pode tirar a empresa de sua

[41] TOP500.org, "TOP500 November 2020".

[42] Strumpf, "Huawei's 5G Dominance Threatened by U.S. Policy on Chips - WSJ".

[43] US-DoC, "Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List | U.S. Department of Commerce".

posição dominante na corrida 5G, e até mesmo dificultar a manutenção de outras redes telefônicas de última geração fornecidas pela empresa e já em uso em diversos países[44]. Os Estados Unidos consideram, adicionalmente, bloquear o fornecimento de tecnologia dos EUA para cinco empresas chinesas de vigilância por vídeo[45].

Como se pode imaginar, restrições à exportação não se aplicam apenas ao hardware, mas também ao software. A proibição do governo dos EUA à Huawei impede a Google de licenciar o uso do sistema operacional Android em aparelhos da empresa[46]. Ocorre que o núcleo do Android é de código aberto e, portanto, pode continuar sendo usado pela empresa chinesa. Não obstante, vários serviços associados são fornecidos pela Google e não estarão mais disponíveis, limitando a utilidade dos smartphones produzidos pela empresa[47].

Em meio ao embargo dos EUA ao fornecimento de tecnologia à China, Pequim ordenou que todos os escritórios do governo e instituições públicas removam equipamentos e softwares estrangeiros até 2022[48]. A medida faz parte de uma campanha para reduzir a dependência chinesa de tecnologias estrangeiras, provavelmente terá um efeito de dissociação das cadeias de suprimentos dos EUA e da China, e poderá ser um

---

[44] Strumpf, "Huawei's 5G Dominance Threatened by U.S. Policy on Chips - WSJ".

[45] Shidong, "China offers five-year tax breaks to chip makers, software developers to bolster industry as trade war stretches to tech".

[46] Moon, "Exclusive: Google suspends some business with Huawei after Trump blacklist - source - Reuters".

[47] Moon.

[48] Yang e Liu, "Beijing orders state offices to replace foreign PCs and software".

duro golpe para as empresas dos EUA[49]. As novas sanções impostas aumentaram a urgência do projeto chinês. Diferentemente dos esforços anteriores de autossuficiência em tecnologia, o objetivo é que em breve as empresas e o governo daquele país fiquem livres das ameaças dos EUA[50].

Não obstante o empenho governamental, a substituição de hardware e software dos EUA por equivalentes chineses também apresenta problemas. A Lenovo, gigante Chinesa de computadores pessoais, usa processadores e discos rígidos da Intel fabricados pela sul-coreana Samsung[51]. A China fica atrás dos EUA em algumas das tecnologias mais avançadas, incluindo design e fabricação de chips. A Intel e a Qualcomm fabricam os principais componentes usados por algumas das maiores empresas de tecnologia do país. Os sistemas operacionais mais utilizados em dispositivos fabricados na China são o Google Android, em smartphones e tablets, e o Microsoft Windows, em computadores[52].

Portanto, ainda que as restrições de exportação de software possam existir, e devam se intensificar no futuro próximo, são mais facilmente contornáveis que aquelas postas à exportação de hardware.

---

[49] Yang e Liu.

[50] Yang e Liu.

[51] Yang e Liu.

[52] Shidong, “China offers five-year tax breaks to chip makers, software developers to bolster industry as trade war stretches to tech”.

2.4.8 "*Data Is the New Oil*" (Dados São o Novo Petróleo)[53]

Por fim, mas não menos importante, há o fato de que na economia criativa da era pós-industrial, o software torna-se parte cada vez mais relevante das expressões científico-tecnológica, econômica e militar do poder nacional.

> Alphabet (a empresa-mãe do Google), Amazon, Apple, Facebook e Microsoft – parecem imparáveis. Elas são as cinco empresas listadas mais valiosas do mundo. Seus lucros estão aumentando: coletivamente, acumularam mais de US$ 25 bilhões em lucro líquido no primeiro trimestre de 2017. A Amazon captura metade de todos os dólares gastos online nos Estados Unidos. Google e Facebook responderam por quase todo o crescimento da receita em publicidade digital nos Estados Unidos no ano passado.[54]

Além das empresas mencionadas, outras como Uber, sem possuir automóveis, e AirBnB, sem possuir imóveis, operam softwares que lhes permitem atuar como intermediários entre proprietários e usuários e ganhar dinheiro com isso. Outros aspectos econômicos da indústria de software são debatidos no terceiro volume desta coleção[55].

Depreende-se que, nas economias modernas, a posse de bens materiais se torna cada vez menos importante, mas a capacidade de conectar grandes quantidades desses recursos com os interessados em disporem deles, em tempo real, se torna cada vez mais relevante.

---

[53] The Economist, "The world's most valuable resource is no longer oil, but data".

[54] The Economist, tradução livre.

[55] Malagutti, *Ciberdefesa e Cibersegurança: Um Olhar Brasileiro*.

2.5 Conclusão

Existem várias razões pelas quais um aspirante a ciberpotência deva se concentrar no Poder de Software em vez de no Poder de Hardware. É bastante improvável que um país que planeje desenvolver cibercapacidades avançadas possa fazê-lo em todas as camadas de software mostradas neste capítulo, pelo menos no curto prazo. Por exemplo, o código do firmware de muitos dispositivos de hardware pode ser inacessível, bem como o código dos *kernels* de muitos sistemas operacionais comerciais e dos *middlewares* usados como base para a construção de sistemas de informação, como gerenciadores de banco de dados, dados e servidores de aplicativos. Isso pode, sem dúvida, limitar a possibilidade de se obter controle total e autossuficiência completa do ciberespaço nacional ou mesmo do mercado de software. Mas existem alternativas, como a adoção de softwares de código aberto, que permitem abreviar o processo de assimilação do conhecimento e reduzir os riscos do uso de "software caixa-preta" (a exemplo de *backdoors* não documentadas). Alcançar o conhecimento avançado ao menos nos níveis superiores do software usado garante uma escala muito menor de risco cibernético e uma "superfície de contato" muito menor, em um ritmo muito mais rápido e com menor custo do que tentar competir no nível do hardware.

Página intencionalmente deixada em branco.

3 Ciberofensas Patrocinadas por Estados

Nas sociedades pós-industriais computadores são ubíquitos e pervasivos. E interconectados. Enquanto essas características atribuem produtividade e interação socioeconômica sem precedentes, elas também apresentam riscos nunca dantes enfrentados. Ciberofensas introduzem a ameaça de que nações poderosas, seja na expressão militar ou naquela econômica, sejam confrontadas por estados muito mais fracos, ou mesmo por protoestados ou grupos terroristas. Ao mesmo tempo, cibersuperpotências desenvolvem a habilidade de, remota e sub-repticiamente, coagir oponentes sem a necessidade de empregar tropas no teatro de operações tradicional. Este capítulo delineia as ameaças postas por ciberofensas patrocinadas por estados e analisa suas características, descrevendo suas aplicações à luz de alguns conceitos militares tradicionais, bem como suas motivações, a natureza de suas *operações*, dos *guerreiros* e das *armas* usadas.

3.1 Introdução

Os perpetradores de cibercrimes, genericamente chamados de hackers, foram divididos em quatro grupos diferentes: cibercriminosos (por vezes subdivididos em indivíduos e crime organizado), hacktivistas, terroristas e estados-nação. Cada um desses grupos tem diferentes motivações, escopo de ações, metas e recursos e, portanto, opções de deterrência e dissuasão[1]. Embora seja claramente possível admitir que qualquer um desses grupos possa ser patrocinado por Estados e usado em uma estratégia de escalada para desestabilizar um Estado oponente, este capítulo se

[1] Malagutti, “O Papel da Dissuasão no Tocante a Ofensas Cibernéticas”.

concentra nas ameaças diretas que os Estados-nação apresentam aos seus pares, considerando suas motivações, a natureza de suas operações, e os guerreiros usados até agora. A análise das ciberarmas é feita em outro capítulo.

3.2 As Motivações

Os Estados-nação têm muitos motivos para perpetrarem ciberofensas. O caso Snowden revelou alguns. O primeiro foi a espionagem política, relacionada às comunicações pessoais dos Presidentes do Brasil e do Mexico, da Chanceler alemã e de alguns de seus ministros, entre milhares de outros indivíduos. Fora do âmbito político, Snowden também revelou a espionagem da Petrobras, empresa estatal brasileira de petróleo, que alguns anos antes anunciara a descoberta de enormes reservas de petróleo em águas brasileiras [2]. Uma terceira motivação real se conecta à segurança e defesa por meio da vigilância, com coleta em massa de metadados sobre chamadas telefônicas, e-mails, mensagens, transferência de arquivos e muitos outros métodos de comunicação[3]. Todos esses exemplos estão relacionados à coleta de informações de inteligência (*intelligence gathering*).

Além dos motivos apresentados, relacionados aos "tempos de paz", existem também as tradicionais motivações militares de "projeção de poder" e "negação de área" no ciberespaço. É improvável que as ciberofensas perpetradas com as tecnologias existentes causem vítimas em massa diretamente [4]. No entanto, elas ainda podem servir como

---

[2] Greenwald, *No place to hide: Edward Snowden, the NSA and the surveillance state*.

[3] UK-GCHQ, *HIMR Data Mining Research Problem Book*; HM Government, "Operational Case for Bulk Powers"; Greenwald, *No place to hide: Edward Snowden, the NSA and the surveillance state*.

[4] Rid, *Cyber War Will Not Take Place*; Rid e McBurney, "Cyber-Weapons".

"meios eficazes de coação política ou força bruta"[5]. Influência e coação de um Estado-nação oponente, por meio de sabotagem, se não um ato de guerra, foi o objetivo do Stuxnet[6].

E depois há... ganho financeiro! Até muito recentemente, essa motivação sempre esteve relacionada apenas aos cibercriminosos, e não aos Estados. No entanto, uma série de ataques contra a rede SWIFT foi associada à Coreia do Norte[7].

A seguir, cada uma das motivações acima é explorada em maior profundidade.

3.2.1 Coleta de Informações de Inteligência

Para os propósitos deste livro, considera-se a coleta de inteligência dividida em duas áreas: "vigilância", a coleta e análise "passiva" de informações, e "espionagem", como a área "ativa".

3.2.1.1 Vigilância

A Inteligência das Comunicações (frequentemente referida como COMINT) sempre desempenhou um papel importante em questões de segurança e defesa. O imperador romano Júlio César (100 AC a 44 AC) já usava um algoritmo de cifragem por transposição, para evitar que seus inimigos entendessem as mensagens capturadas[8].

---

[5] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", 403.

[6] Davis, "Deterrence, Influence, Cyber Attack and Cyberwar"; Falliere, Murchu, e Chien, "W32.Stuxnet Dossier"; TED Talks, *Ralph Kangner: Cracking Stuxnet, a 21st-century cyber weapon*; Sanger, "Obama ordered wave of Cyberattacks against Iran"; Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History".

[7] Perlroth e Corkery, "North Korea linked to digital attacks on global banks".

[8] Singh, *The Code Book: The Secret History of Codes and Code Breaking*, 14–20.

Uma função particular do COMINT é a inteligência de sinais (SIGINT). A agência responsável por essa atividade no Reino Unido (Government Communications Headquarter - GCHQ), define SIGINT como "inteligência derivada de sinais interceptados"[9]. Ela se tornou cada vez mais relevante desde o advento do telégrafo. O GCHQ destaca a importância da interceptação do famoso Telegrama Zimmerman como uma das principais razões para os Estados Unidos terem entrado na Primeira Guerra Mundial[10]. As comunicações por rádio tornaram a SIGINT ainda mais importante, e o GCHQ também aponta a história de Bletchley Park, onde, em 1941, Alan Turing e sua equipe criaram o "Bombe", o primeiro computador da história. Embora eletromecânico, ele ajudou a decifrar o código Enigma usado pelas forças armadas nazistas. Apenas dois anos depois, no mesmo local, a equipe de Tommy Flowers criou o Colossus Mark I, o primeiro computador eletrônico, que decifrou o código ultrassecreto da Lorenz, muito mais complexo, utilizado pelo Alto-Comando Nazista. Ambos foram ativos essenciais para a vitória aliada na Segunda Guerra Mundial[11]. Toda a estrutura operacional de Bletchley Park foi baseada em "SIGINT passivo", com a interceptação e transcrição de todas as mensagens enviadas pelos alemães (interceptação ou coleta em massa), para posterior análise e decifração. Assim, uma operação de vigilância.

A história também mostra que a DARPA patrocinou a criação das fundações da Internet. O processo de SIGINT passivo baseado na Internet hoje em dia é bastante semelhante ao da Segunda Guerra Mundial[12]. Nos últimos anos, "a Internet

---

[9] UK-GCHQ, *HIMR Data Mining Research Problem Book*.

[10] UK-GCHQ, "GCHQ History".

[11] UK-GCHQ.

[12] UK-GCHQ, *HIMR Data Mining Research Problem Book*.

é uma importante fonte de poder de inteligência comparável hoje"[13]. Para a NSA ficou ainda mais fácil, pois

> À medida que a Internet se desenvolveu, uma grande parte do backbone da Internet passou pelos Estados Unidos, o que significa que muitas comunicações estrangeiras poderiam ser acessadas por vigilância feita dentro dos EUA. Anteriormente, as comunicações estrangeiras eram acessadas fora dos EUA, onde a Constituição dos EUA e várias leis são menos rígidas do que para acesso dentro dos EUA.[14]

3.2.1.2 Espionagem

No contexto cibernético, no entanto, a coleta de inteligência não é apenas uma tarefa passiva. O governo do Reino Unido apresentou recentemente ao Parlamento um caso para manter seus poderes em massa concedidos pelo *Investigatory Powers Act 2000*, não apenas para interceptação em massa, mas também para interferência em massa[15]. Em seu *Código de Prática para Interferência de Equipamento*, há uma lista de atividades permitidas quando há "risco para a segurança do Reino Unido"[16]:

> a) obter informações do equipamento em busca de requisitos de inteligência;
>
> b) obter informações sobre a propriedade, natureza e uso do equipamento em busca de requisitos de inteligência;
>
> c) localizar e examinar, remover, modificar ou substituir o hardware ou software do equipamento que seja capaz de fornecer informações do tipo descrito em a) e b);

---

[13] Omand, "Understanding digital intelligence and the norms that might govern it", 2.

[14] Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013", 18, tradução livre.

[15] HM Government, "Operational Case for Bulk Powers".

[16] HM Government, "Equipment interference code of practice pursuant to section 71 of the regulation of Investigatory powers act 2000", 7, tradução livre.

> d) habilitar e facilitar a atividade de vigilância por meio do equipamento.

É importante observar que essas atividades não precisam ser "direcionadas" (*targeted*) a um determinado computador, dispositivo ou mesmo usuário. Elas podem ser realizadas em conjuntos de equipamentos, por exemplo, em um prédio ou vila inteiro, em qualquer lugar do mundo, se houver suspeita de um "risco para a segurança do Reino Unido" nessa "área".

Sua contraparte, a NSA dos EUA, recebeu o direito legal (pela lei americana) de espionar 193 países. A exceção são seus parceiros Five Eyes (Austrália, Canadá, Nova Zelândia e Reino Unido), considerados "fora dos limites" pelo Tribunal de Vigilância de Inteligência Estrangeira sob a Lei de Vigilância de Inteligência Estrangeira de 1978[17].

Da mesma forma, a Suprema Corte dos EUA concedeu ao Federal Bureau of Investigations (FBI) a possibilidade de hackear computadores em todo o mundo, com base apenas em mandados emitidos por juízes americanos. Até então, um juiz em um estado dos EUA só poderia dar ordens limitadas a esse estado[18]. Uma das missões do FBI é contrainteligência[19]. Assim, para defender os EUA contra e espionagem, o FBI está legalmente autorizado a hackear computadores fora dos EUA.

Que informações são visadas pela ciberespionagem? Podem ser informações políticas, militares ou econômicas de (ou sobre) outro governo; ou roubo de segredos comerciais ou propriedade intelectual de empresas privadas ou universidades[20]. O roubo de tecnologia militar a partir de

---

[17] Kedmey, "Report: NSA authorized to spy on 193 countries".

[18] Yadron, "Supreme court grants FBI massive expansion of powers to hack computers"; Khandelwal, "U.S. Supreme court allows the FBI to hack any computer in the world".

[19] https://www.fbi.gov/about-us/investigate/counterintelligence

[20] Cilluffo, Cardash, e Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strenght", 4.

universidades norte-americanas por meio de ciberoperações não é novidade, com um caso famoso relatado já em 1989 por Clifford Stoll em seu seminal *The Cuckoo's Egg (O Ovo do Cuco)*[21]. De fato, nos estágios iniciais da Internet.

A intenção clara da espionagem econômica é "aumentar a prosperidade econômica ou a viabilidade das empresas em um determinado estado" e, embora dirigida pelo estado, seus "beneficiários finais podem ser entidades privadas ou semiprivadas"[22].

O governo dos EUA frequentemente acusa a China de "roubar" informações técnicas, militares e econômicas. Autores americanos argumentam na mesma direção, dizendo que "serviços de inteligência estrangeiros" se envolvem em espionagem industrial em apoio a empresas privadas e que "uma quantidade de propriedade intelectual muitas vezes maior do que toda a propriedade intelectual contida na Biblioteca do Congresso" é roubada a cada ano "de redes mantidas por empresas, universidades e agências governamentais dos EUA" ou que, como o poder nacional está intimamente ligado à vitalidade econômica, perdas sustentadas de propriedade intelectual supostamente poderiam corroer o poder dos EUA[23].

Outros casos recentes mostram que os EUA não são a única vítima dessa atividade. O serviço de inteligência norueguês acusou publicamente os chineses de roubar dados confidenciais e segredos militares estatais de empresas sediadas na Noruega[24]. O governo suíço acusou os russos de

---

[21] Stoll, *The cuckoo's egg: Tracking a spy through a maze of computer espionage*.

[22] Cilluffo, Cardash, e Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strenght", 13.

[23] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy", 100.

[24] Murdock, "Cyber-espionage: Norway's intelligence chief accuses china of stealing military secrets".

estarem conectados à ciberespionagem da empresa fornecedora militar estatal RUAG[25]. Os alemães acusam os russos de estarem por trás dos ataques ao Bundestag[26].

No entanto, um relatório do Parlamento Europeu divulgado em 1999, e os fatos revelados no caso Snowden em 2013, mostraram que a NSA também está envolvida em espionagem econômica ganhando "enorme vantagem para a indústria americana"[27].

Os objetivos finais da espionagem "incluem o desejo de influenciar decisões e afetar o equilíbrio de poder (regional, internacional e assim por diante)"[28].

De fato, durante as recentes eleições presidenciais dos EUA, a comunidade de inteligência dos EUA atribuiu à Rússia o hacking das contas de e-mail de membros do Partido Democrata e o vazamento de informações selecionadas de forma a favorecer o candidato republicano, declarando que os russos pretendiam influenciar os resultados das eleições presidenciais americanas[29]. No dia seguinte, o Presidente Obama afirmou que a Casa Branca estava estudando respostas "proporcionais", enquanto no dia seguinte o Sr. Sergei Lavrov, ministro das Relações Exteriores da Rússia, disse à CNN "não negamos", mas "não vimos um único fato", uma "única prova"; "se eles decidirem fazer algo, deixe-os fazer"[30]. O

---

[25] GovCERT.ch, "APT case RUAG technical report".

[26] Wagstyl, "Germany points finger at Kremlin for cyber attack on the Bundestag".

[27] Campbell, *Development of Surveillance Technology and Risk of Abuse of Economic Information Part 2/5*; Greenwald, *No place to hide: Edward Snowden, the NSA and the surveillance state*.

[28] Cilluffo, Cardash, e Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strenght", 4.

[29] Paletta, "U.S. Blames Russia for recent hacks".

[30] Krever e Smith-Spark, "Lavrov denies Russian influence over US election".

candidato republicano acabou vencendo, embora totalizando mais de um milhão de votos a menos que a candidata democrata. Apenas uma semana após as eleições nos EUA, o chefe da inteligência alemã anunciou que a Alemanha estava preocupada com uma possível influência russa nas eleições alemãs[31].

3.2.2 Militaria

Em 1993, logo após o fim da Guerra Fria, Arquilla e Rondfeld declararam "A ciberguerra está chegando"[32]. A partir de então, o debate sobre o que seria (ou não seria) ciberguerra, ciberarmas e "domínio cibernético" ganhou cada vez mais espaço no imaginário popular, na mídia, na formulação de políticas e na academia.

Nesse "frenesi", há considerações sobre os efeitos diretos ou indiretos de um ciberataque em termos de letalidade ou dano físico a pessoas, máquinas ou prédios, que podem caracterizar o uso da violência[33]. Há discussões sobre o ciberespaço como o quinto domínio de combate, depois de terra, mar, ar e espaço[34]. O debate envolve considerações estratégicas e conceituais, questionando se a ciberguerra não faria parte da guerra de informação ou guerra eletrônica, ou se não seria considerado apenas um multiplicador de forças percorrendo todos os outros domínios[35]. Houve também

---

[31] Wagstyl, "German security head warns of election interference from Russia"; Deutsche Welle, "German intelligence services 'alarmed' about potential Russian interference in elections".

[32] Arquilla e Ronfeldt, "Cyberwar is coming!"

[33] Clarke e Knake, *Cyber war: The next threat to national security and what to do about it*; Mahnken, "Cyberwar and Cyber Warfare"; Stone, "Cyber war will take place!"; Rid, *Cyber War Will Not Take Place*.

[34] Libicki, "Cyberspace is not a Warfighting Domain"; US-JCS, "Information Operations - Joint Publication 3-13".

[35] Kopp, "The Four Strategies of Information Warfare and their Applications"; Stone, "Technology and war: A Trinitarian analysis";

algumas considerações mais metafísicas, como o fato do ciberespaço ser feito pelo homem enquanto os quatro domínios anteriores da guerra anteriores foram criação divina, debate felizmente já superado[36].

Deixando de lado essas discussões, o fato é que a crescente propagação de sistemas computacionais e de informação nas forças armadas modernas tem simultaneamente "empoderado e ameaçado" as forças militares[37]. Para entender como, é útil analisar o papel da cibernética em algumas das funções militares básicas.

3.2.2.1 Projeção de Poder e Negação de Área

Na ciência política e no jargão militar, a "projeção de poder" consiste na capacidade de aplicar o poder nacional fora das fronteiras nacionais. Exemplos militares tradicionais incluem porta-aviões e mísseis balísticos. Mais recentemente, os *drones* se tornaram outro exemplo popular.

É razoável conceber que um ciberataque (CNA) possa ser usado por um país para projetar força sem colocar fisicamente forças militares convencionais no teatro de operações, com custos menores e sem risco de baixas[38].

De sua parte, a "negação de área" refere-se a negar ao adversário a possibilidade de trazer suas capacidades operacionais, ou de usá-las livremente, na região contestada[39]. Exemplos tradicionais podem ser campos minados, arames

---

Mahnken, Lord, e Sharp, *Cyber War and Cyber Warfare*; Sharma, "Cyber wars: A paradigm Shift from Means to Ends"; US-JCS, "Information Operations - Joint Publication 3-13".

[36] Denning, "Rethinking the Cyber Domain and Deterrence"; Libicki, "Cyberdeterrence and Cyberwar".

[37] Arquilla, "From Blitzkrieg to Bitskrieg: The Military Encounter with Computers", 60.

[38] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War".

[39] Russell, "Strategic anti-access/area denial in cyberspace".

farpados ou os "dentes de dragão" usados na famosa Linha Siegfried.

Como implementar negação de área no ciberespaço? Uma resposta imediata parece ser desligar a Internet! Como mencionado anteriormente, a criação da Internet foi patrocinada pela DARPA, uma agência de fomento a pesquisas militares dos EUA. Durante a Guerra Fria, os militares dos EUA estavam preocupados com os riscos de um primeiro ataque nuclear da URSS destruir a capacidade de retaliação dos EUA. Para tanto, a solução foi um desenvolvimento de um sistema projetado para resiliência a esse tipo de ataque.

> Embora grande parte da infraestrutura física do ciberespaço seja relativamente desprotegida, localizada em praias, ao longo de ferrovias e em edifícios em áreas densamente povoadas, muito pouco dessa infraestrutura crítica é crítica por si só. Os nós e cabos podem estar relativamente expostos e potencialmente vulneráveis, mas nenhum é singularmente importante para todo o sistema.
>
> A infraestrutura consiste em cabos e satélites redundantes para comunicações do setor privado e operações militares. A programação lógica dos dados e telecomunicações foi projetada para se adaptar às mudanças de circunstâncias, para direcionar automaticamente o tráfego através de uma rota alternativa quando a primeira rota não estiver disponível. Essa propriedade de "autocura" do ciberespaço torna difícil causar danos substanciais sem lançar um ataque total contra a infraestrutura.[40]

Assim, um ataque visando a destruição da infraestrutura física do ciberespaço em um país bem conectado é praticamente impossível.

Além disso, como já dito, o ciberpoder pode ser dividido em duas categorias: "poder de software" e "poder de hardware". Conforme explicado, destruir o hardware pode ser

[40] Russell, 165.

ineficaz para projetar poder. No entanto, considerando a perspectiva do Software Power, não é necessário destruir o hardware para alcançar a projeção de poder ou a negação de área.

Um bom exemplo das capacidades do Software Power foi fornecido pelo exercício *Eligible Receiver*, promovido pelo Estado-Maior Conjunto dos EUA em junho de 1997 para testar as defesas de computador dos EUA. O cenário proposto era o de uma crise que teria obrigado Washington a enviar tropas e aviões para a Coreia do Sul rapidamente. Trinta e cinco especialistas da Agência de Segurança Nacional (NSA) compuseram a "equipe vermelha"[41], simulando hackers a serviço da Coreia do Norte, que buscavam subverter a operação norte-americana utilizando apenas equipamentos e informações publicamente disponíveis, acessíveis em um conflito real. Em apenas duas semanas, usando somente computadores comerciais e programas de hackeamento baixados da Internet, eles conseguiram "invadir simultaneamente as redes elétricas de nove cidades americanas e quebrar seus sistemas de emergência 911"[42]. Estabelecido o "caos civil e tendo distraído Washington", os hackers atacaram as redes de computadores do Pentágono e tiveram acesso a 36 delas, podendo "circular livremente pelas redes, semeando destruição e desconfiança por onde passassem"; por exemplo, direcionando suprimentos para destinos errados, e possivelmente incapacitando caças a jato de última geração devido à falta de combustível, peças de reposição ou munição[43].

---

[41] No jargão militar ocidental o *red team* (equipe vermelha) geralmente representa o oponente desafiante, enquanto o *blue team* (equipe azul) representa o próprio país.

[42] Adams, "Virtual Defense".

[43] Adams.

Como os hackers promoveram seus ataques remotamente, sem acesso físico (ou de proximidade) aos alvos, eles projetaram poder. Além disso, como limitaram as capacidades operacionais das forças militares dos EUA, impuseram negação de área. Sem destruição física, já que as redes ainda estavam lá. No entanto, os militares dos EUA não podiam mais confiar nessas redes.

3.2.2.2 Interrupção (*Disruption*) e Multiplicação de Força

Existem outros dois conceitos fundamentais no tocante aos usos das cibercapacidades militares. O primeiro diz respeito à ciberguerra estratégica, no sentido da capacidade de provocar grandes efeitos com total surpresa. O segundo se refere à ciberguerra operacional, usada em apoio aos meios militares convencionais em batalha [44].

A ciberguerra operacional tem o potencial de amplificar as operações cinéticas, e é relativamente barata. Vale a pena desenvolvê-la, embora não seja apenas uma questão de técnica, requerendo também a compreensão de como os potenciais oponentes usam as informações para travar suas guerras [45] . Exemplificando as cibercapacidades operacionais, supostamente os chineses dispõem de uma forma engenhosa para inserir vírus de computador pelo ar em três modelos de aviões de reconhecimento e vigilância usados pela Força Aérea dos EUA. Eles realizariam o ataque por meio de ondas eletromagnéticas direcionadas aos sistemas de vigilância a bordo que emitem um sinal específico, o que pode atrapalhar os controles do avião e causar sua queda[46].

De fato, é improvável que os ciberataques sejam decisivos *per se*. O dano (ou interrupção) causado por um ciberataque bem-sucedido provavelmente será mais efêmero

[44] Arquilla, "From Blitzkrieg to Bitskrieg: The Military Encounter with Computers".

[45] Libicki, "Cyberdeterrence and Cyberwar", xx.

[46] Harris, *@War: The rise of the Military-Internet complex*, 63.

do que o de um ataque cinético, pois os defensores podem recuperar os sistemas afetados em relativamente pouco tempo. Outrossim, o maior benefício da ciberguerra provavelmente virá de seu uso em conjunto como (ou como facilitador de) meios militares cinéticos convencionais, como Israel fez na *Operação Pomar* (*Operation Orchard*) em 2007, desabilitando momentaneamente o sistema de defesa aérea sírio enquanto uma esquadrilha de aeronaves de ataque bombardeava as supostas instalações nucleares sírias em Deir ez-Zor e matando uma dezena de técnicos norte-coreanos que apoiavam os sírios[47].

Outra consideração importante envolve Comando-e-Controle (C2). C2, mesmo para muitas capacidades militares não-cibernéticas é tão fortemente dependente do ciberespaço que um oponente pode ser tentado a buscar um primeiro ciberataque incapacitante das forças inimigas[48]. Talvez o efeito mais significativo de *Eligible Receiver* tenha sido o fato de que os hackers também conseguiram paralisar o sistema C2 humano com alto nível de desconfiança originado por ordens falsas de um general comandante, "notícias falsas sobre a crise e instruções de autoridades civis de comando".

> Como resultado, ninguém na cadeia de comando, do presidente para baixo, podia acreditar em nada. Esse grupo de hackers usando recursos disponíveis publicamente foi capaz de impedir que os Estados Unidos travassem uma guerra efetivamente.[49]

---

[47] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War"; Mahnken, Lord, e Sharp, *Cyber War and Cyber Warfare*; Rid e McBurney, "Cyber-Weapons"; Follath e Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor - DER SPIEGEL".

[48] Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm", 62.

[49] Adams, "Virtual Defense", 101.

Este processo é geralmente referido como "decapitação", destinado a perturbar a coesão interna do adversário, e que poderia potencialmente paralisar as forças militares de defesa do Estado atacado e aumentar a eficácia de um ataque cinético subsequente[50].

Uma maneira de evitar a decapitação das cibercapacidades de retaliação é descentralizá-las, e tanto os militares chineses quanto os americanos, tradicionalmente focados no comando centralizado, parecem estar trabalhando no desenvolvimento de cibercapacidades descentralizadas. A China está desenvolvendo cibercapacidades militares em algumas de suas unidades de milícias que compõem o segundo nível de reservas de suas forças militares, normalmente designadas para tarefas locais de defesa civil[51]. Os EUA também planejam empregar seu segundo nível de reservas, a Guarda Nacional, em ciberatividades[52].

A cibernética oferece claramente um novo conjunto de recursos a serem usados pelos estrategistas militares para alcançar fins políticos, seja como multiplicadores de força, incapacitando o inimigo como preparação para ataques cinéticos, ou como ferramentas coativas estratégicas a serem usadas em substituição a ataques cinéticos. Americanos, russos, chineses, franceses e alemães, entre outros, publicaram suas estratégias de defesa, incluindo ciberoperações como parte de suas capacidades e missões militares. O Brasil, penúltimo país do G-20 a publicar sua estratégia de cibersegurança, deliberadamente não inclui a ciberdefesa na mesma.

---

[50] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War".

[51] Austin, "Strategic culture and Cyberspace: Cyber militias in peacetime?"

[52] Shalal, "U.S. National guard may join cyber offense against Islamic state: Carter"; Austin, "Strategic culture and Cyberspace: Cyber militias in peacetime?"

3.2.3 Coação

O anonimato proporcionado pelo ciberespaço também possibilita uma estratégia de coação flexível, permitindo que a medida coativa seja conduzida de forma privada e a vítima responda às ações com "menos preocupação com a influência de terceiros ou as demandas de atribuição conclusiva"[53].

Coação foi o objetivo do Stuxnet, por meio de sabotagem, se não um ato de guerra[54]. Pela primeira vez (conhecida) uma ferramenta de software foi usada por um estado-nação para impor sua vontade política a outro, usando violência, como destruição física de máquinas, e até mesmo letalidade direta, posto que usado contra um interesse vital de uma nação. Assim, em termos "clausewitzianos"[55], um ato de guerra. Ciberguerra. O Stuxnet "conseguiu interromper e atrasar os esforços nucleares iranianos, de acordo com alguns relatos, rivalizando com os possíveis efeitos de um ataque militar limitado"[56]. Stuxnet pode ter sido a opção dos EUA para evitar um ataque aéreo israelense contra as instalações iranianas em Natanz, semelhante ao da *Operação Orchard*[57].

Informações recentes mostram que o Stuxnet era a ponta de lança de uma operação muito maior chamada *Nitro Zeus*, "concebida para desativar as defesas aéreas do Irã, sistemas de comunicação e partes cruciais de sua rede

---

[53] Hare, "The significance of attribution to cyberspace coercion: A political perspective", 138.

[54] Falliere, Murchu, e Chien, "W32.Stuxnet Dossier"; TED Talks, *Ralph Kangner: Cracking Stuxnet, a 21st-century cyber weapon*; Sanger, "Obama ordered wave of Cyberattacks against Iran"; Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History".

[55] Clausewitz, *On War*; Howard, *Clausewitz: A Very Short Introduction*.

[56] Kissinger, *World Order*, 345.

[57] Mazzetti e Sanger, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict".

elétrica[58]. Desde que o Irã assinou um acordo de controle nuclear, o Nitro Zeus "foi engavetado, pelo menos no futuro próximo"[59]. Se a intenção de compelimento do Stuxnet não tivesse sido bem-sucedida, uma gama mais ampla de ciberataques teria sido desencadeada, em uma escalada ainda dentro do domínio cibernético. Isso exemplifica uma mudança gradual do efeito multiplicador de força tática para a ciberguerra estratégica[60].

Não foram apenas os norte-americanos a usarem o ciberpoder para sabotagem (ou *cybotage*). Em dezembro de 2016, uma falta de energia na Ucrânia foi provocada por uma série de ciberataques atribuídos à Rússia, provocados por malwares conhecidos como *Industroyer* ou *CrashOverride*. Apesar de não serem complexos em estrutura, os ataques foram bem coordenados, deixando mais de 80.000 pessoas sem energia por várias horas, no frio inverno ucraniano[61].

3.2.4 Ganhos Financeiros

Até muito recentemente, ganho financeiro sempre foi considerado um objetivo dos cibercriminosos, e não dos estados-nação. Uma série de ataques à rede SWIFT, um consórcio bancário com sede em Bruxelas que administra o que é considerado o sistema de mensagens de pagamento mais seguro do mundo, no entanto, foi atribuído à Coreia do Norte pela empresa de segurança Symantec. Os ataques foram realizados por meio de bancos nas Filipinas, Vietnã e Bangladesh. Mesmo pesquisadores de segurança experientes

[58] Mazzetti e Sanger.

[59] Mazzetti e Sanger.

[60] Sharma, "Cyber wars: A paradigm Shift from Means to Ends".

[61] Zetter, "Everything We Know About Ukraine's Power Plant Hack".

declararam nunca ter visto ataques realizados por um estado-nação para roubar dinheiro[62].

Posteriormente, um relatório da ONU teria indicado que a Coreia do Norte obteve dois bilhões de dólares com o uso de ciberataques, principalmente por meio de *ransomware*[63], usados para obter fundos para seus programas nuclear e de mísseis, contornando as pesadas sanções econômicas impostas ao país justamente por conta desses dois programas[64]. Por conseguinte, cibermeios são efetivamente usados para fins estratégicos por aquele país.

3.3 As Operações

Os exemplos apresentados anteriormente caracterizam ciberoperações. Elas são genericamente denominadas *Computer Network Operations* (CNO) e podem ser divididas em três subconjuntos: *Computer Network Exploitation* (CNE), *Computer Network Attack* (CNA) e *Computer Network Defense* (CND)[65]. Esses tipos de CNO e suas características são detalhados a seguir.

As CNO para coleta de informações e espionagem são frequentemente chamadas de CNE. Um tipo diferente de CNO é denominado CNA e visa "destruir ou incapacitar redes inimigas" ou a confidencialidade, integridade e

---

[62] Perlroth e Corkery, "North Korea linked to digital attacks on global banks".

[63] Software que criptografa arquivos do sistema e cobra resgate, em geral em criptomoedas de difícil rastreamento, para prover a chave de decriptação dos mesmos.

[64] Nichols, "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report | Reuters"; "North Korea: Missile programme funded through stolen crypto, UN report says".

[65] Klimburg e Tirmaa-Klaar, "Cybersecurity and Cyberpower : Concepts , Conditions and Capabilities for Action Wihtin the EU", 7.

disponibilidade (a tríade CIA[66], do acrônimo em inglês) das informações nas redes alvo[67]. É importante observar que a grande diferença entre a CNE e a CNA diz respeito ao seu objetivo (seus efeitos), pois "tecnicamente falando, a CNA exige que a CNE seja efetiva, [que cause efeitos ou danos]. Em outras palavras, o que pode ser uma preparação para a ciberguerra pode ser inicialmente ciberespionagem – ou simplesmente se disfarçar como tal"[68]. Tanto CNE quanto CNA são operações ofensivas e consistem, basicamente, em hackear as redes de computadores do oponente[69].

O último grupo de CNO, e o único defensivo, chama-se CND, e visa defender as redes de computadores tanto de CNE quanto de CNA.

Entre as características mais citadas dos CNOs estão:

- Sua assimetria em comparação com armas convencionais ou nucleares.
- A dificuldade de atribuição e a possibilidade de "negação plausível".
- A vantagem ofensiva decorrente da dificuldade da CND efetiva.
- A dificuldade de dissuadir ciberataques.

3.4 Os Ciberguerreiros

Voltando à questão de Sir Lawrence Freedman[70] sobre "um exército de magos de software usar meios eletrônicos

---

[66] *Confidentiality*, *Integrity* e *Availability*.

[67] Schneier, "Computer Network Exploitation vs. Computer Network Attack".

[68] Klimburg e Tirmaa-Klaar, "Cybersecurity and Cyberpower : Concepts , Conditions and Capabilities for Action Wihtin the EU", 7.

[69] Schneier, "Computer Network Exploitation vs. Computer Network Attack".

[70] Freedman, *Strategy: A history*.

insidiosos para deslocar os sistemas de apoio das sociedades modernas", é interessante também analisar quem integra esse "exército de magos de software".

As operações ofensivas são essencialmente atividades de hackers. O perfil de um hacker se encaixa no da "ideologia da violação" que "sustenta que as coisas que é possível roubar merecem ser roubadas, e a segurança das coisas que são guardadas deve ser testada até a destruição por aqueles com conhecimento técnico suficiente fazer isso"[71].

3.4.1 Hackers

Hackers são, por definição, pessoas que ultrapassam os limites do uso comum das coisas. À medida que esse perfil, associado às capacidades técnicas necessárias foi se tornando popular, ele foi se ajustando à nova realidade.

> Progressivamente, o hacking tornou-se mais objetivamente carregado de propósito. [...] Criminosos cooptaram hackers para fins criminosos; os governos os cooptaram para fins de Estado, incluindo espionagem e guerra; e hackers, como indivíduos humanos, se ligaram voluntariamente a todos os tipos de movimentos sociais e causas por capricho ou convicção.[72]

Os hackers podem "estar fora da folha de pagamento do governo, mas ligados a uma facção política específica ou a políticos individuais (mais provavelmente em estados não ocidentais)" [73]. Eles também podem ser "superpatriotas" sem conexão formal com seu governo, mas "atacando adversários no lugar, ou antes de, onde eles têm certeza de que seu governo faria" ou até agindo como representantes de seus governos[74]. No entanto, os ciberguerreiros são hackers empregados pelo

---

[71] Betz e Stevens, *Cyberspace and the state: Towards a strategy for Cyberpower*, 34, tradução livre.

[72] Betz e Stevens, 33.

[73] Libicki, "Cyberdeterrence and Cyberwar", 46.

[74] Libicki, 46.

Estado, talvez mesmo vestindo uniforme, e agindo "pela causa de objetivos políticos específicos", que podem "ser empregados para criar e operar malware, como o worm Stuxnet"[75].

Enquanto os hackers privados são mais propensos a "usar técnicas que circulam por toda a comunidade hacker", "hackers estatais podem explorar um esforço de pesquisa maior e mais secreto que pode consolidar descobertas, ferramentas e técnicas em sua própria organização". Eles também provavelmente serão "disciplinados em atacar certos alvos por certos motivos e evitar outros que possam parecer igualmente interessantes, mas não fazem parte do plano"[76].

3.4.2 Preto, Branco e Mais de 50 Tons de Cinza

Os hackers são classificados de acordo com o tipo de hackeamento (*hacking*) que praticam. Os "chapéus brancos" (*white hats*) ou "hackers éticos" (*ethical hackers*) são aqueles não mal-intencionados que "exploram redes para seu próprio prazer ou testam sua segurança em nome de seus proprietários", que ganham a vida "descobrindo falhas nos sistemas e depois alertando o fabricante ou desenvolvedor para que eles possa ser remendado". Já os "chapéus pretos" (*black hats* ou *crackers*) são hackers maliciosos que invadem sistemas para propósitos escusos ou maliciosos[77]. Como o mundo não pode ser definido em "preto e branco", existem ainda os "chapéus cinzas", hackers que, embora violem leis ou padrões éticos típicos, geralmente não tem a intenção maliciosa usual de um chapéu preto. O termo popularizou-se a

---

[75] Betz e Stevens, *Cyberspace and the state: Towards a strategy for Cyberpower*, 26.

[76] Libicki, "Cyberdeterrence and Cyberwar", 47.

[77] Betz e Stevens, *Cyberspace and the state: Towards a strategy for Cyberpower*, 25; Harris, *@War: The rise of the Military-Internet complex*, 67.

partir do final da década de 1990, derivado dos conceitos de hackers chapéu branco e chapéu preto.

Outra diferença entre eles está em seus métodos de descoberta de vulnerabilidades. O chapéu branco invade sistemas e redes a pedido de seu contratante ou com permissão explícita para determinar o quão seguro eles são. O chapéu preto invade qualquer sistema ou rede para descobrir informações confidenciais para fins ilícitos. O chapéu cinza geralmente tem as habilidades e a intenção do chapéu branco, mas invadirá qualquer sistema ou rede sem permissão e, ao encontrar uma vulnerabilidade tentará negociar uma recompensa com o proprietário do software para informar os detalhes que permitam sua correção, sem divulgá-la a terceiros. No entanto, como eu costumo dizer, há bem mais de "50 tons de cinza" nesse universo. Nesse espectro, os cinza-claros, não conseguindo a recompensa pretendida, podem vir a informar o proprietário ou fabricante do software assim mesmo, em diferentes níveis de detalhe. Os cinza-médios, ao não conseguirem seu prêmio, não comunicarão nem ao proprietário, nem a ninguém mais, ou talvez o façam parcialmente. Já os cinza-escuros, sentindo-se ignorados, não explorarão a vulnerabilidade diretamente (não são chapéus pretos), mas venderão a informação para terceiros que a explorarão.

3.4.3 Recrutamento e Treinamento

O recrutamento de ciberguerreiros pelas forças armadas dos EUA e pela NSA é muito abrangente. Cada ramo das forças armadas desenvolveu um conjunto de testes de aptidão "para determinar se alguém pode ser adequado para manutenção e defesa de rede ou se mostra promissor para as missões ofensivas mais raras e sofisticadas". Eles também inseriram treinamento básico em cibersegurança para todos os oficiais, enquanto todas as "cinco academias de serviço militar agora incluem a ciberguerra como campo de estudo". Os

melhores hackers de cada um participam de uma competição patrocinada pela NSA, cujos especialistas atuam como uma equipe vermelha para testar suas habilidades. O passo final na "educação dos ciberguerreiros é o treinamento no trabalho"[78].

Os militares também "instaram faculdades e universidades a ensinar ciberguerra", e a NSA trabalhou em conjunto com algumas universidades para ajudar a redigir seu currículo. Em alguns casos, os alunos candidatos precisam passar por uma verificação de antecedentes e obter uma autorização de segurança, uma vez que "parte do curso inclui seminários classificados na NSA", que em alguns casos até oferecem bolsas de estudos e mensalidades para estudantes de ciência da computação que após a graduação tem que trabalhar para a NSA. Os cursos de graduação desenvolvem as habilidades básicas e de defesa. A agência então complementa o treinamento para operações ofensivas[79].

O recrutamento acontece mesmo nos níveis de graduação. Um programa chamado *CyberPatriot*, uma competição nacional para estudantes do ensino fundamental e médio, patrocinado pelos militares e copatrocinado por empreiteiros de defesa, ajuda a identificar jovens talentos na área. "A NSA também recruta nas melhores escolas de ciência da computação, incluindo a Stanford University e a Carnegie Mellon. Além disso, envia representantes para as convenções anuais de hackers mais importantes, Black Hat e DefCon Las Vegas."[80]

O GCHQ britânico, por meio do National Cyber Security Centre (NCSC), por seu lado, trabalha na acreditação de cursos buscando permitir que "estudantes e empregadores possam avaliar a qualidade oferecida e identificar o curso que melhor se adapta à carreira preferida" dentre as diversas

---

[78] Harris, *@War: The rise of the Military-Internet complex*, 61.

[79] Harris, 66.

[80] Harris, 67.

universidades britânicas que oferecem cursos de cibersegurança. Em fins de 2021 o NCSC tinha certificado formalmente ou provisoriamente 39 cursos de mestrado, 2 mestrados integrados (graduação + mestrado), 9 cursos de graduação, e 2 estágios integrados[81].

3.5 Ameaças Persistentes Avançadas (*Advanced Persistent Threats* – APTs)

Esta seção apresenta um grupo particular de ameaças, geralmente perpetradas por Estados, que vem sendo sistematicamente mais referenciada na literatura especializada.

3.5.1 Definição

O termo Ameaça Persistente Avançada (*Advanced Persistent Threats* – APTs) foi supostamente criado em 2007 pelo Coronel Greg Rattray, da Força Aérea dos EUA, para "caracterizar os adversários emergentes que precisávamos lidar em conjunto com a base industrial de defesa"[82]. O termo tornou-se popular após o jornal The New York Times ter publicado detalhes do ataque que sofreu ao longo de ao menos 4 meses, em 2013, atribuído a hackers chineses[83]. Pouco depois a empresa de cibersegurança Mandiant publicou seu relatório que "expunha" uma unidade militar chinesa, a PLA Unit 61398, sediada em Xangai, como "APT1", tendo utilizado e-mails de *spear-phishing* e uma grande quantidade de malwares personalizados para invadir a rede de computadores do influente jornal[84].

---

[81] UK-GCHQ/NCSC, "NCSC-certified degrees".

[82] TAO Security, "Greg Rattray Invented the Term Advanced Persistent Threat".

[83] Perlroth, "Chinese Hackers Infiltrate New York Times Computers".

[84] Mandiant, "APT1 Exposing One of China's Cyber Espionage Units".

Embora não exista uma única definição amplamente aceita de APT, uma definição bastante completa, e de redação complexa, é provida pelo NIST/CSRC dos EUA:

> Um adversário com níveis sofisticados de expertise e recursos significativos que lhe permitem, por meio do uso de vários vetores de ataque diferentes (por exemplo, cibernéticos, físicos e diversivos) gerar oportunidades para alcançar seus objetivos, que normalmente são estabelecer e estender bases dentro da infraestrutura de tecnologia da informação das organizações para fins de exfiltrar continuamente informações e/ou minar ou impedir aspectos críticos de uma missão, programa, ou organização, ou colocar-se em uma posição para fazê-lo no futuro; além disso, a ameaça persistente avançada persegue seus objetivos repetidamente por um longo período de tempo, adaptando-se aos esforços de um defensor para resistir a ela, e com determinação para manter o nível de interação necessário para executar seus objetivos. [85]

Já conforme a Encyclopedia Britannica, APTs seriam

> ataques a ativos de informação de segurança nacional ou importância econômica estratégica de um país, por meio de ciberespionagem ou cibersabotagem. Esses ataques usam tecnologia que minimiza sua visibilidade à rede de computadores e sistemas individuais de detecção de intrusões de computadores. Os APTs são direcionados contra alvos industriais, econômicos ou governamentais específicos para adquirir ou destruir conhecimento de importância militar e econômica internacional. (Stuxnet, por exemplo, se enquadraria nessa definição como um APT dirigido contra o Irã.)[86]

Como se depreende, a primeira definição apresenta APTs como os perpetradores, os sujeitos das ações, e a

---

[85] NIST-CSRC, "advanced persistent threat (APT) - Glossary | CSRC", tradução livre.

[86] Mendell, "advanced persistent threat | information technology | Britannica", tradução livre.

segunda as apresenta como as ações em si mesmas. A lógica da APT como sujeito é também compartilhada pela Mandiant e pela Deloitte[87]. Já a segunda linha de pensamento é também adotada pela Cisco, gigante norte-americana do setor de redes de computadores[88]. Por sua vez, a Kaspersky, uma empresa referência em cibersegurança, reconhece ambas as possibilidades[89].

Independentemente da discussão quanto a ser o sujeito que comete a ação ou a ação propriamente dita, o conceito pode ser melhor entendido pela decomposição de seus elementos constituintes, o que fazemos nas próximas subseções.

3.5.1.1 Ameaça

APTs constituem ameaças por apresentarem tanto capacidade quanto intenção. Os ataques de APTs são caracterizados por ações humanas coordenadas, e não processos aleatórios ou automatizados. Os perpetradores têm um objetivo específico e são qualificados, motivados, organizados e bem financiados.

3.5.1.2 Persistente

Os perpetradores têm objetivos específicos de longo prazo, e não buscam um acesso de oportunidade a informações para ganhos imediatos. Tal característica indica que as APTs são guiadas por demandas exógenas aos grupos em si mesmos. Os ataques são realizados a longo prazo, em geral por meio de monitoramento e interação contínuos voltados a alcançar os objetivos definidos. Dessa característica decorre que seus ataques não são constituídos de processos repetitivos e atualizações frequentes de malware, para escapar à detecção.

---

[87] Mandiant, “APT1 Exposing One of China’s Cyber Espionage Units”; Rieder, “Advanced Persistent Threat”.

[88] CISCO, “What Is an Advanced Persistent Threat (APT)?”

[89] Kaspersky, “What Is an Advanced Persistent Threat (APT)?”

Outrossim, uma APT é um "grupo não-oportunista que viola organizações de forma estratégica e de longo prazo com objetivos claros", que "não serão facilmente dissuadidos em suas ações até que tenham alcançado o que se propuseram a fazer[90]. Uma vez que um APT tenha entrado em seu alvo, o ataque pode durar meses ou anos; ou seja, é uma ameaça "persistente". O motivo por trás da ameaça vai além do mero ganho político ou financeiro. APTs não praticam hacktivismo (penetrar em um site ou rede para fazer uma declaração política), nem cibercrime no sentido estrito, no qual criminosos roubam informações apenas para obter lucro. Em vez disso, o objetivo é ganhar vantagem estratégica ou tática no cenário internacional[91].

A métrica *dwell time* (algo como "tempo de residência" ou "permanência"), o tempo em que um ataque APT passa desapercebido (ou o tempo decorrido entre a infecção e a remediação), tem se reduzido significativamente ao longo dos anos, com a média tendo caído de 416 dias em 2011 para 24 dias em 2020[92]. Quanto mais longo este tempo, maior a probabilidade de os atacantes completarem o ciclo de ataque, propagarem sua ação e alcançarem seus objetivos.

3.5.1.3 Avançada

Os perpetradores que integram (ou praticam) APTs têm um amplo espectro de meios de inteligência à disposição, que podem incluir o aparato de inteligência de um estado, como ativos de inteligência humana (HUMINT), infiltração e engenharia social para obter acesso a instalações físicas de forma a viabilizarem seus ciberataques, para então instalarem malware personalizado para a instituição alvo.

---

[90] Rieder, "Advanced Persistent Threat".

[91] Mendell, "advanced persistent threat | information technology | Britannica".

[92] FireEye/Mandiant, "M-Trends 2021 Report".

Embora alguns componentes dos ataques possam não ser considerados particularmente "avançados", como componentes de malware comumente disponíveis, ou o uso de materiais de exploração facilmente adquiridos, os perpetradores podem acessar e desenvolver ferramentas mais avançadas conforme se faça necessário. Eles geralmente combinam múltiplos métodos, ferramentas e técnicas de segmentação, a fim de alcançar e comprometer seu alvo e manter o acesso a ele. Os operadores também podem demonstrar um foco deliberado na segurança operacional que os diferencia de ameaças "menos avançadas".

3.5.2 Modus Operandi

Entendidos os conceitos fundamentais e as divergências conceituais, passemos à discussão dos elementos sobre os quais há pouca divergência.

APTs são pouco intuitivas. Quando se pensa em hackers geralmente se imagina que seu objetivo seja contaminar o máximo de computadores possíveis e que quanto mais computadores sejam infectados, maiores as oportunidades de se roubar dinheiro, obter benefícios e atingir quaisquer que sejam seus objetivos[93].

Mas uma APT é (ou realiza) um ciberataque furtivo a uma rede de computadores específica, buscando ganhar e manter acesso não autorizado e permanecer sem ser detectado por um período significativo, no qual o perpetrador frequentemente monitora, intercepta e transmite (ou exfiltra) informações e dados confidenciais, em vez de causar uma paralisação da rede, negação de serviço ou infecção com malwares destrutivos.

Seria óbvio o interesse na instalação de um *keylogger* ou *backdoor* na máquina de um alto dirigente de uma importante instituição privada ou governamental. Além disso,

[93] Kaspersky, "What Is an Advanced Persistent Threat (APT)?"

eles frequentemente possuem equipes e ferramentas de cibersegurança para protegê-los. Outrossim, ao invés de tentar atacar diretamente os altos-executivos, APTs costumam visar pessoal de menor escalão, provavelmente sem acesso a nenhuma informação valiosa, mas que compartilha a rede com máquinas importantes, e assim pode ser usado como "trampolim" para se atingir o objetivo final[94].

Os APTs geralmente usam táticas de engenharia social ou exploram vulnerabilidades de software em organizações com informações de alto valor[95]. O *spear-phishing* usa e-mails enviados para funcionários selecionados dentro de uma organização. Os e-mails parecem vir de fontes confiáveis ou conhecidas. Seja clicando em links dentro do e-mail ou sendo persuadidos pela aparente legitimidade do e-mail para baixar a guarda, esses funcionários permitem que programas hostis entrem em seus computadores. O malware de zero-day é um software de computador hostil, como vírus ou cavalos de Tróia, que ainda não é detectável por programas antivírus. Redes de computadores já comprometidos, conhecidos como "botnets", distribuem esses ataques de zero-day. Nenhum dos métodos é novo, e eles não são exclusivos de APTs. Seu uso contra ativos de segurança nacional, no entanto, é indicativo de um ataque APT em vez de hackers convencionais[96].

Em 2013, a Mandiant identificou um ciclo de vida similar para os ciberataques de APTs chinesas supostamente realizados entre 2004 e 2013, constituído pelos seguintes passos[97]:

1) Compromisso inicial: realizado por meio de engenharia social e *spear-phishing*, por e-mail, e

---

[94] Kaspersky.

[95] CISCO, "What Is an Advanced Persistent Threat (APT)?"

[96] Mendell, "advanced persistent threat | information technology | Britannica".

[97] Mandiant, "APT1 Exposing One of China's Cyber Espionage Units".

utilizando malware zero-day. Outro método de infecção comum era o implante de malware em um sítio que os funcionários da vítima provavelmente visitariam.

2) Estabelecimento de Base (Comando e Controle): implante de software de administração remota na rede da vítima, criação de backdoors e túneis de rede que permitissem acesso furtivo à sua infraestrutura.
3) Aquisição (ou Escalação) de Privilégios: uso de explorações e quebras de senha para aquisição de privilégios de administração do computador infectado e possivelmente sua expansão para contas de administração da rede.
4) Reconhecimento Interno: coleta de informações sobre a infraestrutura ao redor, relacionamentos de confiança e estrutura da rede.
5) Movimento Lateral: expansão do controle para outras estações de trabalho, servidores e elementos de infraestrutura e a coleta de dados neles residentes.
6) Manutenção da Presença: garantia do controle contínuo sobre os canais de acesso e credenciais adquiridas em etapas anteriores.
7) Missão Cumprida: exfiltração de dados roubados da rede da vítima.

3.5.3 Motivação e Alvos

As motivações de APTs são tipicamente políticas ou econômicas. Seus alvos mais comuns incluem agências governamentais, fornecedores de equipamentos de defesa e indústrias que desenvolvem tecnologias de importância estratégica militar ou econômica, como empresas

aeroespaciais e de computadores[98]. Itens específicos para exfiltração de dados incluem e-mails, documentos, segredos comerciais e bancos de dados com informações confidenciais, bem como projetos de produtos, listas de fornecedores, notas de laboratórios de pesquisa e resultados de testes[99].

Dentre os setores mais visados, destacam-se:

- Agronegócio
- Defesa
- Energia
- Ensino Superior e Centros de Pesquisa
- Finanças
- Tecnologia
- Telecomunicações
- Transporte
- Saúde

Suspeita-se que governos e estados-nação usem APTs para a obtenção de informações sobre operações militares ou de inteligência específicas, bem como a sabotagem de operações de interesse de defesa, dos quais alguns exemplos seriam Titan Rain, Ghostnet, Stuxnet e Putter Panda. Além disso, grupos menores estão usando ferramentas mais simples, como engenharia social, para ter acesso e roubar propriedade intelectual[100].

3.5.4 Proteção

Como já visto, os ataques APT são por natureza furtivos e podem usar softwares mais sofisticados do que ferramentas comuns de hackeamento "de prateleira" (*off-the-shelf*) encontradas na Internet. Sua "pegada" em um

---

[98] Mendell, "advanced persistent threat | information technology | Britannica".

[99] Mendell.

[100] CISCO, "What Is an Advanced Persistent Threat (APT)?"

computador ou rede é relativamente pequena, e os APTs tentam operar abaixo do nível de detecção de um sistema de detecção de intrusões (IDS).

Tecnologia e métodos tradicionais de segurança têm sido ineficazes na detecção ou mitigação de APTs. Quando as organizações detectam lacunas em sua segurança, elas intuitivamente implantam um produto específico para preencher essa lacuna. Uma solução repleta de produtos específicos, no entanto, continuará a ter lacunas inerentes ao processo como um todo[101]. Para se evitar tais lacunas na segurança, as organizações precisam adotar uma abordagem holística, que requer uma solução de segurança multicamadas e integrada trabalhando em conjunto é a melhor maneira de aumentar a segurança[102].

No campo da prevenção, considerando que a grande maioria dos ataques de APTs se inicia com pessoal de menor escalão da instituição alvo, cada vez mais companhias investem na educação de seus funcionários [103]. Essa educação passa a ser mais comumente denominada ciber-higiene, consistindo no ensino de um conjunto de práticas voltadas a garantir que a utilização de redes de computadores com menos problemas e na identificação de potenciais ameaças como e-mails de phishing [104].

No campo da detecção, a descoberta de uma infecção por uma APT é possível por meio do monitoramento detalhado do tráfego em uma rede. A identificação das comunicações entre o botnet mestre (a base de C2) e o malware implantado revela o comprometimento (ou a invasão) do sistema. Esta

---

[101] CISCO.

[102] CISCO.

[103] Kaspersky, “What Is an Advanced Persistent Threat (APT)?”

[104] Damião, “Ciberhigiene: a base da saúde de uma organização”.

necessidade de atividade de C2 permanece sendo o calcanhar de Aquiles das APTs. [105]

A defesa cibernética ativa tem gerado maior eficácia na detecção, atribuição e eliminação/neutralização de APTs, ao também utilizar elementos do aparato de inteligência estatal no combate às ameaças cibernéticas para atividades de caça e perseguição aos adversários.

3.6 Conclusão

Uma análise criteriosa da literatura disponível sobre ciberpoder, em sua maioria escrita por autores de países afiliados à OTAN, mostra que ela reflete uma postura agressiva, baseada na necessidade de ferramentas de ataque que podem tanto incutir medo quanto impor domínio no ciberespaço. Além disso, as evidências apresentadas tanto pelos casos Snowden e Stuxnet, como também Nitro Zeus, como a dos demais casos analisados, corroboram essa percepção.

Até o momento há poucos atos conhecidos de cibersabotagem ou ciberataques com fins militares interestatais. Mas há muitos relatos de casos de espionagem, com a subjacente ameaça de influência e interferência no processo tomada de decisão. Os atores estatais dominantes até agora são os membros do grupo Five Eyes (EUA, Reino Unido, Austrália, Canadá e Nova Zelândia) e Coreia do Norte, Índia, Israel, Irã e França, frequentemente citados no polo ativo das ciberofensas.

Na economia globalizada dos dias de hoje, todas as nações podem ter interesses conflitantes com pelo menos um dos países citados. Em particular uma nação com a proeminência econômica internacional do Brasil. Assim, há a necessidade de proteger esses interesses tendo em mente o

[105] Mendell, “advanced persistent threat | information technology | Britannica”.

ciberpoder, e a intenção de usá-lo, desses atores. Isso requer preparação, planejamento e investimentos de longo prazo, típicos em questões de segurança e defesa nacional.

4 Ciberarmas

4.1 Introdução

A literatura está repleta de diferentes denominações de ciberarmas: vírus, vermes (*worms*), *botnets*, Cavalos de Tróia (*Trojans*), *malware*, código trapaceiro (*rogue code*), bombas lógicas, e assim por diante. Mas todas elas têm duas coisas em comum: consistem em software (*Software Power*!), e necessitam ser de alguma forma implantadas previamente nas redes alvo. Um implante é um software construído para ativar e possibilitar uma ação subsequente: em muitos casos, ele permite que o atacante envie (ou carregue) código de ataque que o sistema alvo executará, causando danos em sua funcionalidade ou integridade[1].

Neste capítulo nos deteremos mais detalhadamente nas características das armas cibernéticas.

4.2 A "Natureza" Única das Ciberarmas

As ciberarmas apresentam uma característica distinta em relação ao armamento convencional. Para os outros domínios da guerra (terrestre, aéreo, marítimo e espacial) a distinção entre armamentos ofensivos ou defensivos é praticamente inexistente. Em geral, quando as capacidades defensivas se desenvolvem, as ofensivas também o fazem. Por exemplo, um veículo blindado, um avião de combate ou um submarino podem ser usados tanto para defesa quanto para ataque, conquanto possam ser mais adequados para um ou outro fim.

No ciberespaço, no entanto, a distinção entre uma arma ofensiva ou defensiva costuma ser bastante impressionante. De fato, essas armas, no mais das vezes "principalmente

[1] Libicki, "Pulling Punches in Cyberspace", 139.

software", "embora às vezes também hardware", podem ser divididas em três grupos[2]:

a. Armas inequivocamente ofensivas: diferentes tipos de malware (vírus, worms, cavalos de Tróia, bombas lógicas e similares); ações de negação de serviço.

b. Ferramentas de uso duplo: monitoramento de rede; varredura de vulnerabilidades; testes de penetração; criptografia; e camuflagem do conteúdo das comunicações.

c. Ferramentas inequivocamente defensivas: firewall, sistemas de recuperação de desastres.

Portanto, uma "ciberarma" como o Stuxnet será sempre ofensiva, nunca defensiva. Por outro lado, um sistema de detecção de intrusão (IDS) ou antivírus sempre será defensivo, nunca ofensivo. Mesmo o desenvolvimento de sistemas defensivos não exige o desenvolvimento de capacidades ofensivas para testá-los, pois é possível usar as ameaças já existentes e documentadas para testar sistemas defensivos.

Há uma percepção fantasiosa de que "no reino cibernético, a diferença entre uma arma e uma não-arma pode se resumir a uma única linha de código, ou simplesmente à intenção do usuário de um programa de computador"[3]. No entanto, não há nenhuma evidência para apoiá-la. Não se aplica nem mesmo ao grupo "uso duplo" proposto por Tabansky, pois elas estão prontas para serem usadas, e não precisam ter seu código alterado em uma única linha para serem utilizadas para seus fins precípuos.

Poder-se-ía argumentar que uma pequena mudança em uma ferramenta defensiva como um antivírus ou IDS, inserindo uma *backdoor*, poderia facilitar operações ofensivas, diluindo a distinção entre armas ofensivas e defensivas.

[2] Tabansky, "Basic Concepts in Cyber Warfare", 80, tradução livre.

[3] Nye, "Rules of the Cyber Road for America and Russia".

Entretanto, tal *backdoor* seria somente uma vulnerabilidade, não uma arma em si. Ela viabiliza explorações e ataques, mas não os constitui. No mundo cinético, equivale ao conhecimento de uma vulnerabilidade em uma fortificação defensiva ou sistema de radar, por exemplo, que para ser explorada exigirá capacidades ofensivas específicas e adequada preparação. Por exemplo, Eben-Emael, a formidável fortaleza belga, era considerada virtualmente inexpugnável por um ataque frontal. Mas, como a história registra, era vulnerável a um ataque "por cima". Assim, os alemães usaram tropas de assalto aerotransportadas como uma "arma ofensiva" para explorar essa vulnerabilidade, invadindo-a silenciosamente por cima e dominando-a por dentro, em uma missão projetada e treinada especificamente para esse fim. Da mesma forma, apenas uma ferramenta de ataque explicitamente destinada a ser uma ciberarma ofensiva pode explorar uma vulnerabilidade específica. Em outras palavras

> Uma vez dentro, você precisa de uma ferramenta personalizada para criar os efeitos desejados. Muitas vezes, ela tem que ser uma ferramenta artesanal para o alvo específico. Não é o mesmo que fabricar bombas de duzentos quilos e colocá-las na prateleira com seus kits de orientação a laser.[4]

Além disso, as "armas de software" ofensivas (malware) envolvem milhares de linhas de código projetadas para atingir propósitos específicos e explorar vulnerabilidades específicas. E o número de linhas de código está aumentando com a crescente complexidade das ciberarmas. Até 2005, "a maioria das amostras de malware contém alguns milhares de SLOCs [linhas de código-fonte]", com apenas algumas amostras contendo mais de uma dúzia de milhares de SLOCs; a partir de 2007, as contagens estão na faixa de dezenas de milhares: GhostRAT (33.170), Zeus (61.752), KINS (89.460),

[4] Hayden, *Playing to the edge: American intelligence in the age of terror*, 145.

Pony2 (89.758) ou SpyNet (179.682). A maioria das amostras corresponde a malware moderadamente complexo[5]. Mesmo as atualizações de uma versão para outra de um malware podem chegar a 4.600-9.000 linhas[6]. Estima-se que o Stuxnet tenha cerca de 15.000 linhas de código, a maioria escrita em C++, para explorar cinco vulnerabilidades de "dia-0" (*0-day*) e uma vulnerabilidade "não-dia-0"[7].

Quanto às ciberarmas defensivas (antivírus, IDS, firewalls, etc.), elas também constituem projetos de software complexos, e não é razoável supor que seu tamanho seja menor que suas congêneres ofensivas. Mas, em vez de explorar vulnerabilidades, estas buscam por padrões ("indicadores de comprometimento", explicados mais adiante) e controlam o acesso aos recursos computacionais. Portanto, não é plausível supor que mudar "uma única linha de código" alteraria sua natureza. Na verdade, nem mesmo uma *backdoor* simples e direta, e assim facilmente identificável, pode ser implementada com uma única linha de código. E não configura uma mudança de natureza da ciberarma. Apenas abre uma vulnerabilidade potencialmente explorável, como já explicado.

Similarmente, uma linha de código pode provocar um erro ou uma instabilidade no funcionamento do software, e isso pode (ou não) ser descoberto por um hacker e explorado como uma vulnerabilidade. Para serem exploradas, vulnerabilidades demandam softwares complexos, provavelmente com milhares de linhas de código, como exemplificado anteriormente, que possam se aproveitar adequadamente de suas características específicas de uma forma útil ao atacante.

---

[5] Calleja, Tapiador, e Caballero, "A look into 30 years of malware development from a software metrics perspective", 10–11.

[6] Lindorfer et al., "Lines of malicious code: Insights into the malicious software industry", 9.

[7] Falco, "Stuxnet Facts Report", 7; 20.

De outra parte, o raciocínio oposto, no sentido de se transformar um malware ofensivo em software defensivo, é ainda mais difícil de se imaginar possível por meio da alteração de umas poucas linhas de código, e menos ainda de uma única linha.

4.3 Anatomia das Ciberarmas Ofensivas (ou Cadeia Destrutiva Cibernética - *Cyber Kill Chain*)

As modernas ciberarmas ofensivas são ferramentas de ataque multiestágio para a realização de operações de CNE ou CNA, usualmente baseadas na Cadeia Destrutiva das Intrusões (*Intrusion Kill Chain*)[8]. Cada estágio se destina a executar diferentes funções em diferentes momentos. Os sete estágios originais da cadeia destrutiva das intrusões foram rearranjados nos treze passos da Cadeia Destrutiva Cibernética dos Sistemas de Controle Industrial (*Industrial Control Systems* ou ICS) apresentados a seguir[9]:

- Reconhecimento (*reconaissance*): consiste no exame, possivelmente com o suporte de inteligência humana (HUMINT), do alvo, para encontrar possíveis "fraquezas e identificar informação que suporte os atacantes em seus esforços para mirar, explorar e implantar elementos em um sistema".
- Municiamento (*weaponization*): "inclui modificar um arquivo que de outra forma seria inofensivo", como um documento PDF ou MS Word, "com o intuito de permitir o próximo passo do atacante".
- Mira ou Seleção de Alvo (*targeting*); "é o processo de análise e priorização de alvos e adequação das ações

[8] Hutchins, Amin, e Cloppert, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains", 3–7.

[9] Lee e Assante, "The Industrial Control System Cyber Kill Chain", 4–16.

letais ou não-letais apropriadas a esses alvos para criar os efeitos desejados".

- Envio (*deliver*): consiste no atacante encontrar um "método para interagir com a rede do defensor", por exemplo um e-mail de *phishing* utilizado para entregar o PDF "municiado".
- Exploração (*exploit*): "são os meios que o adversário usa para executar suas ações maliciosas", por exemplo quando o PDF "municiado" é aberto.
- Instalação (*install*): é a consequência de uma exploração bem sucedida, por exemplo quando o PDF "municiado" instala o implante ou malware, ou conecta uma VPN.
- Comando e Controle (C2): consiste no estabelecimento de uma conexão pelo implante previamente instalado, por exemplo abusando de comunicações acreditadas como uma VPN, geralmente "se escondendo no tráfego normal de entrada e saída, sequestrando as comunicações existentes".
- Ação (*act*): pode consistir em muitas ações diferentes, sendo as mais comuns: descobrir (e corromper) novos alvos (sistemas aplicativos ou dados); movimentar-se lateral pela rede; instalar e executar capacidades adicionais; exfiltrar dados; implementar técnicas anti-forenses, como a limpeza de rastros da atividade de ataque; e defender o implante ou estabelecer uma posição defensiva ao confrontar defesas ou resposta a incidentes.
- Desenvolvimento e Ajuste (*attack development and tuning*): consiste no desenvolvimento de capacidades sob medida para o alvo específico e para os resultados almejados.
- Teste (*testing*): consiste no teste das capacidades desenvolvidas contra uma instalação de testes tão similar quanto possível ao ambiente alvo, sempre

baseado nas informações coletadas nos passos anteriores.

- Entrega (*delivery*): consiste na entrega das novas capacidades desenvolvidas especificamente para o alvo pretendido.
- Implantação (*installation*): é a instalação (ou atualização) do software antigo pela nova versão com capacidades específicas.
- Execução (*execution*): consiste na execução do implante para atingir os objetivos desejados.

A premissa de defesa deste modelo é a de que "a mitigação de qualquer passo quebra a cadeia e frustra o adversário"[10].

4.4 Indicadores de Comprometimento

Considerando que o software geralmente segue uma determinada sequência de passos, ele tende a se repetir em cada infecção. Consequentemente, qualquer repetição do padrão de ataque é uma fragilidade que os defensores devem reconhecer (identificar) e aproveitar[11]. Esses padrões são conhecidos como "indicadores de comprometimento" (IOCs, da sigla em inglês).

IOCs, portanto, são padrões de comportamento ou "assinaturas deixadas pelo malware (a ciberarma) quando se implanta (instala) ou inicia sua atividade. Podem ser explicados conforme abaixo[12]:

> Por exemplo, o malware EXEMPLO.exe ao ser executado no sistema operacional faz as seguintes atividades:

[10] Hutchins, Amin, e Cloppert, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains", 3.

[11] Hutchins, Amin, e Cloppert, 3.

[12] CTIR Gov, "Indicadores de Comprometimento".

> 1. Cria uma tarefa agendada para iniciar o EXEMPLO.exe com o Sistema Operacional [SO];
>
> 2. Inicia uma conexão de rede utilizando o protocolo TCP com o host 192.0.2.100 na porta 443;
>
> 3. Realiza o download do pacote de ferramentas privesc.msi que possui o hash 58c29cc95eb34e7a88b34ccf426a3494;
>
> 4. Desativa o software antivírus do SO;
>
> 5. A cada 24 horas se conecta com host 192.0.2.100 na porta 443;

Ciberataques são bem-sucedidos, em geral, porque as defesas são usualmente baseadas no reconhecimento de IOCs apenas de alguns desses estágios individualmente, e não do ataque completo.

Em outras palavras, as ferramentas defensivas em geral falham por buscarem IOCs de certos estágios de ataques já conhecidos, mas não são capazes de reconhecer ataques novos ou modificados de malwares derivados das versões anteriores, cujos IOCs serão provavelmente diferentes.

Além disso existem hoje malwares que são "polimórficos". Como o nome indica, eles adotam diferentes formas. Na prática, eles se modificam de forma mais ou menos aleatória, criptografando a si mesmos com uma nova chave a cada infecção, e assim gerando assinaturas (IOCs) distintas, que não são facilmente identificadas pelos softwares de proteção e defesa.

Mais difícil ainda é o caso das ciberarmas "metamórficas", que como o nome indica, modificam não apenas a aparência, mas a forma. Esse tipo de malware vai além, e "pode mudar sua estrutura interna, reescrevendo e reprogramando-se cada vez que infecta um sistema de computadores"[13]. A boa notícia é que a criação de malware

[13] Kaspersky Labs, "O que é vírus metamórfico? | Definição de vírus metamórfico".

desse tipo é extremamente complexa, limitando sua disponibilidade. A má notícia é que essa complexidade não é um obstáculo de muito difícil superação para os recursos de um estado-nação.

4.5 Portas dos Fundos (*Backdoors*)

Implantes podem ser inseridos no software alvo conforme este é desenvolvido, e podem ser usados para criar "interruptores de desligamento" (*kill switches*) e "portas dos fundos" (*backdoors*) remotamente operadas, por exemplo escritas no *firmware* dos *chips* do computador, permitindo que intrusos manipulem remotamente os sistemas neles executados[14].

Já em 2001 oficiais de inteligência americanos acreditavam "que certos equipamentos e softwares importados da Rússia, China, Israel, Índia e França" estavam infectados com "dispositivos" capazes de "ler dados e destruir sistemas", embora essa suspeita fosse difícil de comprovar[15].

Recentemente, no entanto, hardware falsificado foi identificado em sistemas adquiridos pelo Departamento de Defesa dos EUA[16]. Um relatório do Comitê Permanente de Inteligência da Câmara, em 2012, recomendou restrições à aquisição de equipamentos das companhias chinesas Huawei e ZTE[17]. Em dezembro de 2015 a empresa norte-americana Juniper Networks anunciou a descoberta de uma porta dos fundos secreta no sistema operacional de seus firewalls[18]. Não ficou claro quem teria inserido a porta dos fundos no sistema.

---

[14] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy", 101.

[15] Adams, "Virtual Defense", 105.

[16] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy", 97.

[17] Banach, "Investigative report on the U.S. National security issues posed by Chinese telecommunications companies Huawei and ZTE".

[18] Zetter, "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors".

4.6 Agentes Inteligentes

A mais famosa ciberarma até hoje é o Stuxnet, que entre outras características é também "notável por algo que ele não fez": embora um agente "inteligente", ele não era um agente "aprendiz". Técnicas de aprendizado por máquinas vêm sendo rapidamente desenvolvidas e uma nova geração de agentes poderia ser capaz de aprender. De fato, "como as instituições de defesa e inteligência dos EUA, Grã-Bretanha e Israel estiveram tradicionalmente bastante à frente das tendências em pesquisa em ciência da computação", "seria surpreendente se uma arma de software inteligente capaz de aprender ainda não tivesse sido desenvolvida"[19].

Em 2019 o *think tank* britânico IISS argumentou que havia duas razões para que os primeiros sistemas de armas autônomos operados por Inteligência Artificial, que provavelmente seriam norte-americanos, fossem empregados no ciberespaço. A primeira é a de que sistemas de armas cinéticos são muito mais complexos, em razão das necessidades de controle de mobilidade e de combate. A segunda é a de que a maioria dos militares mais graduados da OTAN prefere tratar ciberarmas como auxiliares de seus sistemas cinéticos, e assim o uso de armas autônomas operadas por inteligência artificial no ciberespaço enfrentaria menos resistência interna nas forças armadas desses países.[20]

A mesma lógica de agentes inteligentes pode ser aplicada a sistemas defensivos. Em 2009 o Departamento de Segurança Interna dos EUA publicou um guia para pesquisa em segurança cibernética onde apontava a necessidade de detecção de ameaças baseado em mecanismos de aprendizado para encontrar discrepâncias [21]. Esse tipo de ciberarma

[19] Rid e McBurney, "Cyber-Weapons".

[20] IISS, "Artificial Intelligence and Offensive Cyber Weapons".

[21] US-DHS, "A Roadmap for Cybersecurity Research".

defensiva se encaixa perfeitamente no contexto do que os norte-americanos denominam Ciberdefesa Ativa (Active Cyber Defense – ACD)[22].

4.7 Assimetria

O termo "guerra assimétrica" é por vezes utilizado para caracterizar "o enfrentamento da força adversária focando em suas fraquezas"[23]. Ele se adequa bem à ideia de "inexistência de entrada forçada no ciberespaço", mas simplesmente a exploração das vulnerabilidades do inimigo[24].

Todavia, focar nas fraquezas do adversário seria prudente em qualquer conflito, e não apenas naqueles assimétricos. A melhor definição, portanto, seria considerar assimetria como a disparidade de poder entre os oponentes.

Os custos de desenvolvimento de forças convencionais ou nucleares exercem um efeito dissuasivo, por exemplo, pela futilidade de se competir com a marinha norte-americana na construção de frotas de porta-aviões ou submarinos[25]. A mesma ideia se aplica ao desenvolvimento de defesas por mísseis. Além dos custos, existem dificuldades associadas ao acesso às tecnologias relacionadas, como os tubos de foguetes "sem costuras" feitos com ligas metálicas especiais, necessários à produção de mísseis, e aos componentes necessários à produção e operação de reatores nucleares de pequeno porte para porta-aviões e submarinos nucleares.

Não é difícil imaginar que uma ferramenta similar ao Stuxnet possa ser usada para infectar e desabilitar as defesas de mísseis dos EUA, Rússia, China, Índia ou Paquistão, por exemplo. O Stuxnet danificou as partes eletromecânicas das centrífugas iranianas fazendo-as girarem em velocidades

---

[22] NSA | CSS, "Active Cyber Defense (ACD)".

[23] Adams, "Virtual Defense", 98–99.

[24] Libicki, "Cyberdeterrence and Cyberwar", xiv.

[25] Nye, "Cyber War and Peace"; Rumsfeld, "Transforming the military".

superiores às da operação normal prevista, gerando desgaste nos equipamentos e enganando os sistemas de controle para parecer que o funcionamento estava normal. Efeito similar poderia ser obtido nas turbinas de vapor dos submarinos nucleares. Ou um malware poderia danificar algum componente eletromecânico, preferivelmente de difícil reposição, das plataformas de lançamento de mísseis balísticos. Dessas formas hipotéticas, uma ferramenta cujo custo de desenvolvimento estaria na casa das dezenas de milhões teria inutilizado sistemas militares que custam bilhões. Talvez nem sequer o malware fosse necessário; apenas uma porta dos fundos pudesse incapacitar o sistema de alerta de mísseis ou seu sistema de lançamento por, digamos, meia hora.

Este é o cenário usualmente associado ao conceito de assimetria relacionado ao Software Power, dado que "as barreiras de entrada no domínio cibernético são tão baixas que atores não-Estatais e pequenos Estados podem desempenhar papel significativo a baixo custo"[26].

> A assimetria também é causada pelo desequilíbrio do espaço de ataque - nações maiores e mais dependentes de tecnologia possuem um número maior de redes com muito mais pontos frcos vulneráveis a ataques do que nações com uma menor superfície de redes para proteger.[27]

Isso leva a uma situação onde, mesmo que grandes potências façam maiores investimentos no desenvolvimento de suas capacidades cibernéticas, estados menores ainda têm mais oportunidades de competirem nesse domínio do que naquele de armamentos convencionais, considerando que "na guerra moderna 'massa' não é mais um fator decisivo", e que

[26] Nye, "Cyber War and Peace".

[27] Areng, "Lilliputian States in Digital Affairs and Cyber Security", 6.

"a guerra assimétrica dilui o poder tradicional e a lógica da dominância"[28].

> Mais especificamente, é precisamente por outros sofrerem de inferioridade em conflitos convencionais que eles sentem-se compelidos a enfatizar ciberataques como forma de igualar o placar. Assim, os Estados Unidos, por todas as suas vantagens, pode sofrer mais do que seus adversários sofreriam se a retaliação gerar contraretaliação.[29]

Software Power, então, oferece meios para que "Estados Liliputianos" (bem como atores não-Estatais) desenvolvam suas capacidades e enfrentem oponentes que de outra forma não poderiam ser confrontados[30].

A assimetria proporcionada pelas cibercapacidades ofensivas e sua proliferação pode até criar cenários que "fornecem a potências convencionalmente um deterrente mais forte contra seus adversários mais fortes" [31]. Esse contexto poderia levar a uma situação em que, em vez de guerra, haveria uma resolução negociada de conflitos, com Estados mais fortes oferecendo a seus adversários uma barganha melhor do que eles teriam em outro caso[32]. Para evitar essa possibilidade e manter sua vantagem, Estados com forças convencionais mais fortes investem para manter sua vantagem. No entanto, nações como Irã e Coreia do Norte foram apontadas como detentoras de cibercapacidades relevantes, capazes de criar problemas para os EUA e o Reino Unido.

Sob a ótica da ciberdefesa, a vantagem de potências menores foi capturada pelo no NRI, *Network Readiness Index* (algo como Índice de Prontidão de Redes) de 2015, o qual não

---

[28] Areng, 11.

[29] Libicki, "Cyberdeterrence and Cyberwar", 32, tradução livre.

[30] Areng, "Lilliputian States in Digital Affairs and Cyber Security", 5–6.

[31] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War".

[32] Liff.

mostrou nenhum integrante do G-20 nas cinco primeiras posições, ocupadas por Cingapura, Finlândia, Suécia, Países Baixos e Noruega, com os EUA ficando em sétimo e o Reino Unido em oitavo[33]. A edição de 2021 do NRI apresentou apenas os EUA nas cinco primeiras posições, ocupadas por Países Baixos, Suécia, Dinamarca, EUA e Finlândia[34].

4.8 Efemeridade

Todo o conceito de ferramentas de ciberataque é baseado na exploração de vulnerabilidades. Isso pode ocorrer por meio do municiamento de um arquivo no formato Adobe PDF ou Microsoft Word com código malicioso, ou possivelmente pela exploração de uma porta dos fundos instalada no software de um ativo de rede, como um roteador.

Quando uma vulnerabilidade é informada a um fabricante de software, ele publica correções, ou "remendos" (*patches*), para corrigi-la. Esses remendos são geralmente aplicados por meio de "atualizações de software" (*software updates*). A mesma situação ocorre com sistemas de detecção de intrusão (IDS) e software antivírus (AV). Quando o remendo é aplicado aquela vulnerabilidade específica torna-se inútil para aquele alvo particular, e uma outra precisa ser encontrada.

Claramente, uma exploração pode já ter ocorrido quando o remendo é aplicado, e um implante pode já ter sido instalado no sistema. Não obstante, supondo que esse implante tenha sido desenvolvido para "exfiltrar" [35] dados pelo estabelecimento de uma VPN, por exemplo utilizando privilégios de uma identidade e senha de rede, se essa senha

---

[33] Dutta, Geiger, e Lanvin, "The Global Information Technology Report 2015", 8.

[34] Dutta e Lanvin, "Network Readiness Index 2021", 36.

[35] Usado aqui com o sentido inverso de "infiltrar", significando "extrair clandestinamente".

for alterada cessará a possibilidade do implante executar sua missão.

E enquanto esse implante tentar usar essas credenciais agora inválidas ele poderá revelar-se para os defensores que monitoram a rede, permitindo uma posterior atribuição e seus consequentes efeitos indesejados. Para se evitar esta situação o implante deve ser inteligente o bastante para detectar que suas credenciais não mais são válidas e "cometer suicídio", removendo-se a si mesmo e eliminando seus rastros para evitar ou dificultar a atividade forense.

Em todo caso, ferramentas de ataque são válidas para um cenário bastante específico de vulnerabilidades presentes numa particular combinação de versões de software nas diversas camadas: aplicativos, *middleware*, sistema operacional, "direcionadores", firmware, os próprios IDS e AV, e seus remendos. Uma versão não atualizada de um sistema operacional pode ainda vir a ser protegida (ao menos parcialmente) pela última versão de um AV, e assim por diante.

Uma explicação breve e simples sobre a efemeridade pode ser a seguinte:

> Para atacar um alvo, primeiro você precisa penetrá-lo. Acesso adquirido com meses, se não anos, de esforço, pode ser perdido com uma atualização casual do sistema alvo, nem mesmo um projetado para melhorar as defesas, mas apenas uma atualização administrativa de algo 2.0 para algo 3.0. [36]

Por conseguinte, as ciberarmas são efêmeras em sua natureza, posto que as vulnerabilidades conhecidas podem ser eliminadas por uma série de razões distintas, fora do controle do pretenso atacante. Outrossim, para que uma ciberarma de ataque tenha valor prático, ela precisa ser implantada o quanto antes. E depois de implantada precisa ser verificada de tempos

[36] Hayden, *Playing to the edge: American intelligence in the age of terror*.

em tempos, para assegurar que continue disponível em caso de necessidade.

4.9 Imprevisibilidade e Incontrolabilidade

Ciberarmas são também parte integrante do ciberespaço globalmente interconectado em que estamos imersos. "Os efeitos de ataques em um ponto podem espalhar-se imprevisivelmente, muito além do alvo e até mesmo de volta para o atacante, dada a *natureza altamente interdependente do ciberespaço*"[37].

Um aspecto interessante do Stuxnet é o fato dele ter infectado uma rede apartada (*air gapped*), um sistema não conectado à Internet, indicando a possibilidade do malware ter chegado a seu alvo por meio de uma vasta gama de componentes, que vão de um drive USB infectado até componentes de software e hardware comerciais "de prateleira", como um direcionador (*driver*) *plug-and-play* ou coisa equivalente[38].

O desenvolvimento de armas de software enfrenta um dilema complicado: deveriam seus objetivos ser "largos-e-rasos" (*wide-and-shallow*) ou "estreitos-e-profundos" (*narrow-and-deep*)? Essencialmente, atingir maior potencial destrutivo vai aumentar significantemente a complexidade, e assim o custo e o prazo de desenvolvimento da ciberarma, mas limitar os alvos potenciais e os riscos de danos colaterais e, assim, a "utilidade política" do armamento[39].

Por algum tempo especulou-se que um erro de programação teria permitido que o Stuxnet tivesse "escapado" além dos confins das redes-alvo iniciais. Atualmente, porém,

---

[37] Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm", 61, grifo nosso.

[38] Arquilla, "From Blitzkrieg to Bitskrieg: The Military Encounter with Computers", 62.

[39] Rid e McBurney, "Cyber-Weapons".

acredita-se que sua missão original, a destruição das centrífugas nucleares iranianas, tenha sido mudada numa versão posterior, permitindo que o mesmo realizasse missões de reconhecimento, enviando a seus criadores os endereços IP de máquinas infectadas pelos fornecedores trabalhando para os iranianos. As "características mais agressivas" implementadas nas últimas versões do Stuxnet teriam aumentado as chances dele ser descoberto, como de fato o foi em junho de 2010 por uma pequena empresa da Bielorússia[40]. "Escapado" ou não ele infectou muitos ICSs em mais de 150 países, e agora pode estar sendo redesenhado para outros fins[41]. E esta é, a propósito, uma importante característica das armas cibernéticas: sua acelerada e incontrolável proliferação. Langner, alçado à fama por ter "descoberto" o Stuxnet, chegou a celebrar o fato de que o malware tenha sido desenvolvido pelos EUA[42]; os diversos níveis de controle nele implementados teriam evitado um estrago maior em outros ICSs utilizando o mesmo software (ou similares) da Siemens ao redor do mundo.

4.10 A Dominância Norte-Americana

Durante a Guerra Fria, quando o mundo estava dividido em dois, Brodie [43] definiu os EUA como uma nação *status quo*: "determinada a manter o que tem, incluindo a existência de um mundo cuja metade ou é mais amigável ou ao menos não vivamente e perenemente hostil".

Após a desagregação da União Soviética, os EUA se tornaram uma superpotência inconteste tanto nas forças convencionais quanto nucleares. E continuam ainda uma

---

[40] Harris, *@War: The rise of the Military-Internet complex*, 46–47.

[41] Arquilla, "From Blitzkrieg to Bitskrieg: The Military Encounter with Computers", 64.

[42] TED Talks, *Ralph Kangner: Cracking Stuxnet, a 21st-century cyber weapon*.

[43] Brodie, "The Anatomy of Deterrence", 173, tradução livre.

nação *status quo*, mas agora não apenas no tocante a metade do mundo. De fato,

> [...] Líderes americanos tanto do partido Democrata quanto do Republicano deixaram claro que eles acreditam que os EUA, para citar Madeleine Albright, são a "nação indispensável" e assim têm tanto o direito quanto a responsabilidade de policiar todo o planeta.[44]

A indústria de software norte-americana é a maior do mundo, sendo uma exportadora líquida e concentrando muitos dos melhores programadores do mundo; os cursos de computação de suas universidades são ranqueados no topo, e o Pentágono tem trabalhado em parcerias público-privadas para a criação de capacidades militares superiores no ciberespaço[45]. Embora haja considerável sigilo a respeito das capacidades ofensivas norte-americanas, acredita-se amplamente que estejam entre as melhores do mundo.

Os EUA recentemente incrementaram em 35% (19 bilhões de dólares) seu orçamento para políticas de segurança cibernética, incluindo 3 bilhões para a criação de uma Reserva Cibernética[46]. Eles veem a supremacia no "quinto domínio" como essencial para sua missão, e incorporaram ciberataques à sua doutrina de guerra convencional. Eles os têm usado para incapacitar a infraestrutura de outros países da mesma forma que dizem temer seja feito contra eles domesticamente[47].

A Diretiva Política Presidencial 20 (PPD-20), de 2012, vazada em 2014, "instrui os militares a designarem uma lista de alvos além-mar de 'importância nacional' onde seja mais

---

[44] Mearsheimer, "The gathering storm: China's challenge to US power in Asia", 386, tradução livre.

[45] Libicki, "Cyberdeterrence and Cyberwar"; Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy"; Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm"; Rid e McBurney, "Cyber-Weapons".

[46] Austin, "Strategic culture and Cyberspace: Cyber militias in peacetime?"

[47] Harris, *@War: The rise of the Military-Internet complex*, xxi.

facilmente ou mais efetivamente possível para os EUA atacarem com armas cibernéticas que com aquelas convencionais"[48]. "No espectro das hostilidades os EUA estão no polo agressivo"[49]. As melhores evidências concretas são os casos Stuxnet e Snowden.

4.11 Comparando Armamentos Cinéticos e Cibernéticos

Descritas as características essências da ciberarmas, torna-se possível elaborarmos uma tabela comparativa que apresente de forma resumida as diferenças entre elas e diferentes armas cinéticas. Essa é a proposta da Tabela 4-1.

Considerando nossa ênfase no caso brasileiro, vamos nos ater a armas cinéticas que integram o projeto de modernização das Forças Armadas Brasileiras. No caso da Força Aérea Brasileira (FAB) temos o Saab Gripen F39E/F, caça de 4ª geração (ou 4,5 geração, pois incorpora avanços em relação à 4ª geração, sem no entanto se caracterizar como de 5ª geração), cuja aquisição de 36 unidades foi contratada em 2014 como parte do Programa FX/2, e cuja intenção é chegar a 66 unidades, com transferência de tecnologia sueca para o Brasil[50]. Pela Marinha do Brasil (MB) temos os submarinos da classe S-BR, uma variante da classe Scorpène francesa em desenvolvimento conjunto pelos dois países para a construção de quatro unidades de propulsão convencional e uma quinta de propulsão nuclear[51].

---

[48] US-White House, "Presidential Policy Directive/PPD-20"; Harris, *@War: The rise of the Military-Internet complex*, 54.

[49] Harris, *@War: The rise of the Military-Internet complex*, xxi.

[50] Saab, "Programa Gripen Brasileiro"; Gielow, "FAB compra novos mísseis e quer mais 30 caças Gripen".

[51] Marinha do Brasil, "Submarino Scorpène: A Posição da Marinha"; Galante, "Diferenças entre o submarino Scorpène e o S-BR brasileiro - Poder Naval - Navios de Guerra, Marinhas de Guerra, Aviação Naval, Indústria Naval e Estratégia Marítima".

Tabela 4-1 – Características do Armamentos Modernos

Arma	Ofensiva	Defensiva	Previsível	Controle	Ciclo de Vida	Replicável
Gripen	✓	✓	✓	✓	🚶	✗
S-BR	✓	✓	✓	✓	🚶	✗
Leopard	✓	✓	✓	✓	🚶	✗
Astros 2020	✓	✓	✓	✓	🚶	✗
IA2	✓	✓	✓	✓	🚶	✗
Stuxnet	✓	✗	✗	✗	🤰	✓

Fonte: Elaborada pelo autor.

Pelo Exército Brasileiro (EB) temos um armamento para cada "arma combatente". Pela Cavalaria, temos os carros de combate, popularmente conhecidos como "tanques de guerra", da classe Leopard 1-A5, (tecnologia alemã)[52]. A Artilharia está representada pelo sistema Astros 2020, plataforma de lançamento de foguetes que incorpora o Míssil Tático de Cuzeiro MTC-300, com alcance de 300km e o Foguete Guiado SS-40G, cujo projeto é brasileiro[53]. Já a

[52] Valentini e Dalla Costa, "Leopard 1A5Br - Nova família de blindados sobre lagartas no EB: uma proposta".

[53] Godoy, "Míssil de precisão entra em fase final"; Brasil-MD-EPEX, "Folder Astros 2020".

Infantaria está representada pelo fuzil de assalto Imbel IA2, também de projeto brasileiro[54]. No tocante às ciberarmas, elas estão representadas pelo "velho Stuxnet" (de 2010), que se acredita ser um desenvolvimento conjunto norte-americano e israelense.

A comparação mostra as principais diferenças entre as diversas classes de armamentos, e leva em consideração a natureza ofensiva ou defensiva, a previsibilidade, a controlabilidade, o ciclo de vida e a replicabilidade e adaptabilidade das armas para a criação de novas armas.

Como se depreende, o Stuxnet, enquanto ciberarma, difere das demais em todos os quesitos. Quanto à natureza, todas as demais podem ser aplicadas tanto ofensiva quanto defensivamente; o Stuxnet é a exceção, com aplicação específica para um propósito único. Enquanto as demais são controláveis e previsíveis em seu funcionamento, o Stuxnet não o é, potencialmente afetando alvos distintos daquele pretendido. Enquanto as demais envolvem longos ciclos de vida, de uma ou mais décadas, estima-se que o Stuxnet tenha sido desenvolvido em apenas 2 anos. E isso, por óbvio, afeta seu custo, sendo este o principal componente da assimetria oferecida pelas ciberarmas. Por fim, nenhuma das outras plataformas é facilmente replicável. Já o Stuxnet, em questão de meses, teve partes replicadas e adaptadas para a geração de dois outros malwares: Flame e Duqu[55].

4.12 Conclusão

Este capítulo apresentou as características peculiares das ciberarmas, que fazem com que devam ser consideradas de forma inerentemente diversa daquelas das armas cinéticas (e mesmo estratégicas) até hoje conhecidas e profundamente estudadas.

---

[54] Imbel, "Fuzil de Assalto 7,62 IA2".

[55] Sterling, "Flame/Stuxnet/Duqu are attacking Kaspersky".

Para chegar a tal conclusão, apresentou a natureza única das ciberarmas e explicitou a anatomia das ciberarmas ofensivas, também conhecida como *cyber kill chain* (ou cadeia destrutiva cibernética). Também explicou o conceito de indicadores de comprometimento e seu uso, limitado mas importante, para a identificação de intrusões e vulnerabilidades. Em seguida, expôs o conceito e a importância das *backdoors*, e a necessidade de domínio da maior parte possível dos softwares utilizados para se evitar a presença (e a exploração) delas por parte de adversários.

Adicionalmente, apresentou uma explanação do que são agentes inteligentes, componentes de ciberarmas que começam a se tornar cada vez mais autônomos e a incorporar capacidades de aprendizado, o que os tornará cada vez mais difíceis de detectar e combater.

Seções sucessivas trataram da questão da assimetria provida pelas ciberarmas, no tocante às capacidades convencionais, e trataram também da natureza efêmera, imprevisível e incontrolável das ciberarmas, mostrando que a necessidade de exploração cada vez mais rápida das vulnerabilidades cibernéticas torna tais características cada vez mais perigosas. Depois, abordou-se a questão da dominância norte-americana, e o surgimento e consolidação de outras cibersuperpotências.

Uma última seção traçou uma comparação entre as ciberarmas e outras plataformas de armas em desenvolvimento e aquisição pelo Brasil.

5 Ciberdissuasão

Este capítulo analisa a aplicação, ao ciberespaço, dos conceitos da Teoria da Dissuasão (ou de seu superconjunto Teoria da Causação), conforme identificados em *Dissuasão: Um Olhar Brasileiro* [1]. Seus elementos constitutivos são estudados à luz das diferentes visões que permeiam o debate atual no ambiente acadêmico internacional.

5.1 Introdução

Analisando os escritos da "Teoria da Deterrência", Jervis[2] identificou três "ondas" dessa teoria.

> Embora a primeira onda, que veio e se foi nos primeiros anos da era nuclear, tenha tido pouco impacto, as ideias da segunda onda, que atingiu o auge no final da década de 1950, logo se tornaram sabedoria convencional, embora houvesse pouca evidência para a validade de as proposições. De fato, até a terceira onda", na década de 1970, houve poucos pedidos de verificação.[3]

Em comparação, Nye afirmou que "teorizar sobre dissuasão na era cibernética está emergindo apenas de sua primeira onda"[4]. A pesquisa sobre ciberdissuasão começou já na década de 1990, "alimentada pelo Departamento de Defesa dos EUA em vários exercícios de jogos de guerra"[5]. De 2008 a 2016 o tema cresceu no interesse acadêmico, mas depois esse interesse pareceu evaporar. Dificuldades na aplicação dos

---

[1] Malagutti, *Dissuasão: Um Olhar Brasileiro*.

[2] Jervis, "Deterrence Theory Revisited."

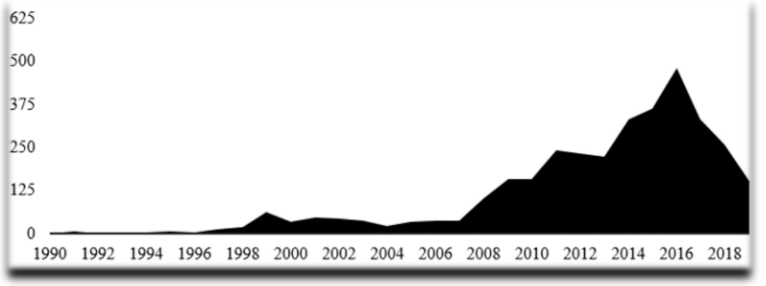
[3] Jervis.

[4] Nye, "Deterrence and Dissuasion in Cyberspace."

[5] Smeets and Soesanto, "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!"

elementos tradicionais de dissuasão, amplamente apresentados na literatura disponível, contribuíram para que o conceito saísse de moda[6].

Figura 5-1 – Evolução do Número de Publicações sobre Ciberdissuasão



Fonte: Smeets e Soesanto[7]

Muitos estados-membros da União Europeia (UE) aderiram à caracterização do ciberespaço dos EUA, como um domínio de guerra que demanda por ciberdeterrência. Embora eles tenham duas grandes preocupações em relação ao conceito dos EUA de Engajamento Persistente. Primeiro, eles o percebem como "excessivamente agressivo"; segundo, eles consideram bastante improvável que as organizações cibernéticas militares europeias possam dispor dos recursos que tal conceito demanda[8]. Devido a essas limitações, alguns autores afirmam que "os estados membros da UE terão que preencher esse vazio estratégico com pensamento conceitual criativo"[9].

A preocupação "eurocêntrica" desses autores pode ser replicada para todas as potências médias não europeias. Ainda

[6] Smeets and Soesanto.

[7] Smeets and Soesanto.

[8] Smeets and Soesanto.

[9] Smeets and Soesanto.

assim, exigirá ainda mais criatividade daqueles que têm tradição não-agressiva, pois, sem poder recorrer ao uso da força devido às suas restrições culturais e institucionais, têm que abrir mão da "ameaça de retaliação", base da maioria dos escritos sobre ciberdissuasão.

A dissuasão no domínio cibernético difere da dissuasão nuclear em alguns aspectos; a cibernética "exige um foco nos atores, em vez de apenas em armas/capacidades; portanto, priorizar esses atores de acordo com o escopo, escala e natureza da ameaça que eles representam é fundamental"[10].

5.2 A Necessidade de Ciberdissuasão

A queda do Muro de Berlim (1989) e o fim da União Soviética (1991) marcaram o fim da Guerra Fria. Com ele, o medo de uma guerra nuclear diminuiu significativamente. Apenas dois anos depois, Arquilla e Ronfeldt[11] declararam "A guerra cibernética está chegando!". Desde então, a a "ciberguerra" ganha cada dia mais espaço no imaginário popular, na mídia, na formulação de políticas e na academia, com debates sobre o que seria uma ciberguerra e se ela ocorreria [12] ou não [13].

Enquanto isso, o avanço da sociedade pós-industrial acelerou a inclusão digital [14]. A rápida expansão da Internet em todo o mundo, tornando os computadores cada vez mais difundidos e onipresentes, criou um novo espaço: o ciberespaço. Também gerou um deslocamento de poder

---

[10] Cilluffo, Cardash, and Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strenght."

[11] Arquilla and Ronfeldt, "Cyberwar Is Coming!"

[12] Clarke and Knake, *Cyber War: The next Threat to National Security and What to Do about It*; Stone, "Cyber War Will Take Place!"

[13] Rid, *Cyber War Will Not Take Place*.

[14] Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*; Toffler, *The Third Wave*.

(Powershift) nas sociedades em todo o mundo e uma Riqueza Revolucionária, com novos meios de produção de bens e serviços [15].

A princípio, o avanço do ciberespaço parecia indicar que as fronteiras nacionais poderiam "esmaecer", assim como a ideia de soberania nacional. Essa percepção foi reforçada pela globalização das operações financeiras, com trilhões de dólares fluindo diariamente pelas redes de computadores, de um "canto" do mundo para outro. No entanto, nos últimos anos, o desenvolvimento do poder cibernético e seu uso agora sugerem que ele está se tornando "apenas" mais uma ferramenta de estadismo (*statecraft*), com amplo uso potencial para influência e coação interestatal. Assim, apresenta-se como objeto de estudo da geopolítica, no sentido de "o estudo da espacialização da política internacional pelas potências centrais e estados hegemônicos"[16].

Portanto, as operações de influência do ciberespaço demandam atenção da academia, dos formuladores de políticas e da sociedade em geral. No entanto, a pesquisa ainda é incipiente, assim como a coleta de evidências empíricas sobre conflitos cibernéticos e tentativas de influência. Assim, "a resposta para a questão de saber se a dissuasão funciona no ciberespaço é 'depende de como, quem e o quê'" [17]. "Ironicamente, dissuadir grandes Estados como a China de atos de força pode ser mais fácil do que dissuadir atores não estatais de ações que não atingem o nível de força"[18].

---

[15] Toffler, *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*; Toffler and Toffler, *Revolutionary Wealth: [How It Will Be Created and How It Will Change Our Lives]*.

[16] Tuathail and Agnew, "Geopolitics and Discourse. Practical Geopolitical Reasoning in American Foreign Policy."

[17] Nye, "Deterrence and Dissuasion in Cyberspace."

[18] Nye, "Can China Be Deterred in Cyber Space?"

5.3 Segurança Nacional e Ciberespaço

A inteligência das comunicações sempre desempenhou um papel essencial nas questões de segurança e defesa. A Inteligência de Sinais (SIGINT) tornou-se cada vez mais relevante com a popularização das telecomunicações, e ainda mais crítica para os militares. Em Bletchley Park, em 1941, Alan Turing e sua equipe criaram o "Bombe", o primeiro computador da história. Embora eletromecânico, ajudou a decifrar o código Enigma usado pelas forças armadas nazistas. Apenas dois anos depois, no mesmo local, a equipe de Tommy Flowers criou o Colossus Mark I, o primeiro computador eletrônico, que decifrou o código ultrassecreto da Lorenz, usado pelo Alto-Comando alemão. Ambos foram ativos essenciais para a vitória aliada na Segunda Guerra Mundial[19].

Além de seu uso para o SIGINT, o processamento automatizado de informações também foi relevante para outras atividades militares. Também em 1943, o exército americano encomendou à Universidade da Pensilvânia o desenvolvimento de uma máquina capaz de computar alvos balísticos, resultando no desenvolvimento do ENIAC, o primeiro computador eletrônico programável, entregue em 1946[20].

O medo da repetição da "blitz", o bombardeio de Londres durante a Segunda Guerra Mundial, em território norte-americano levou à criação do *Semi-Automatic Ground Environment* (SAGE), integrando centenas de estações de radar com processamento em 23 supercomputadores distribuídos pelos EUA, cuja protótipo foi demonstrado já em 1951[21]. O sistema foi contratado pela IBM e utilizou linhas de comunicação comercial da AT&T para integrar toda a rede, ao

[19] UK-GCHQ, "GCHQ History."

[20] Rid, *Rise of the Machines*.

[21] Rid.

custo total (em 15 anos) de mais de 500 bilhões de dólares em valores atualizados. Em 1958, o SAGE foi centralizado no mítico Comando de Defesa Aérea Norte-Americana (NORAD) no Colorado[22]. Da mesma forma, por meio da Agência de Projetos de Pesquisa Avançada (ARPA), o Pentágono financiou o desenvolvimento da ARPANET, a "famosa precursora da Internet"[23]. O objetivo era melhorar os sistemas de comando e controle militares e fornecer redundância de rota no caso de falha de um nó de rede[24].

No Brasil, o desenvolvimento da tecnologia da informação também esteve ligado a interesses militares. Foi por influência das ideias do Tenente Comandante Geraldo Maia, que havia retornado dos EUA, que o Conselho Nacional de Desenvolvimento da Administração do Presidente Kubitscheck propôs a criação de um grupo para avaliar o uso de computadores no país[25]. No ano seguinte, a equipe tornou-se o Grupo Executivo de Aplicação de Computadores Eletrônicos (GEACE) e autorizou a importação dos três primeiros computadores brasileiros: um para a Pontifícia Universidade Católica do Rio de Janeiro; um para o Instituto Brasileiro de Geografia e Estatística (IBGE); e um para a empresa Listas Telefônicas Brasileiras[26].

Em 1972 foi criada a Coordenação de Atividades de Processamento Eletrônico de Dados (CAPRE), vinculada ao Ministério do Planejamento[27]. A CAPRE recebeu a responsabilidade de desenvolver uma política e um programa

---

[22] Rid.

[23] Rid.

[24] Rid.

[25] Moreira, "Informática: O Mito Política Nacional de Informática."

[26] Moreira.

[27] Figueiredo, "Legislação de Informática No Brasil"; Tonooka, "Política Nacional de Informática: Vinte Anos de Intervenção Governamental"; Moreira, "Informática: O Mito Política Nacional de Informática."

nacional de Tecnologia da Informação, e uma de suas primeiras determinações foi a restrição à importação de hardware estrangeiro por instituições governamentais[28]. Uma reserva de mercado de 20 anos acabara de começar. Em 1979 a CAPRE foi substituída pela Secretaria Especial de Informática (SEI), então subordinada ao Conselho de Segurança Nacional, e fortemente influenciada pelo Serviço Nacional de Informações (SNI), agência de inteligência brasileira à época[29].

Em 1984, foi aprovada a Lei de Informática. Ela estabeleceu a Política Nacional de Informática, pela qual somente produtos de hardware e software *Made in Brazil* (ou estrangeiros autorizados) poderiam ser comercializados (semelhante ao *Buy American Act*[30], mas exclusivamente para o mercado de TI). A ideia era criar um mercado voltado para o desenvolvimento de uma indústria nacional que pudesse ser competitiva internacionalmente. O modelo adotado baseou-se em três pilares: capacitação de pessoal; estímulo ao investimento privado; e criação de uma empresa estatal, a Computadores Brasileiros (COBRA). No entanto, tais esforços foram infrutíferos, e até mesmo contraproducentes, haja visto que submeteram o país a um atraso considerável na adoção de novas tecnologias que surgiram rapidamente no mercado externo, mas que não entraram no Brasil, e os altos valores que os usuários nacionais pagaram para produtos em relação aos

[28] Moreira, "Informática: O Mito Política Nacional de Informática"; Figueiredo, "Legislação de Informática No Brasil"; Tonooka, "Política Nacional de Informática: Vinte Anos de Intervenção Governamental."

[29] Moreira, "Informática: O Mito Política Nacional de Informática"; Tonooka, "Política Nacional de Informática: Vinte Anos de Intervenção Governamental."

[30] U.S. Government Accountability Office, "The Buy American Act."

preços internacionais[31]. Em 1993, com o fim da reserva de mercado, as empresas brasileiras optaram pelo licenciamento de produtos estrangeiros.

5.4 Operações de Ciberpoder e Causalidade

O conceito de poder na política e estratégia internacional é de influência (incluindo coação) para mudar o comportamento e as ações dos outros[32]. "Ciberguerra" (ou guerra cibernética), é um termo cativante e se tornou popular, por vezes usado até mesmo pelo Secretário-Geral da ONU[33]. No entanto, caracterizar ciberataques como atos de guerra é bastante difícil à luz dos conceitos e casos atuais. A maioria dos ciberataques patrocinados por Estados retratados na mídia são, de fato, tentativas de influência realizadas por nações contra seus pares, contemporaneamente classificadas como operações de "zona cinzenta" (*gray zone*), projetadas para provocar "causação" (persuasão ou dissuasão), abaixo do limiar das operações usualmente consideradas atos-de-guerra.

Para entender melhor essas operações, é necessário saber como alguns conceitos fundamentais se aplicam (ou são aplicados) no ciberespaço. O primeiro grupo deles não é inerente à Teoria da Causalidade, mas afeta o comportamento dos Estados no ciberespaço. O segundo grupo é o dos conceitos da Teoria da Causação.

---

[31] Moreira, "Informática: O Mito Política Nacional de Informática"; Tonooka, "Política Nacional de Informática: Vinte Anos de Intervenção Governamental."

[32] Singer, "Inter-Nation Influence: A Formal Model"; Betz and Stevens, *Cyberspace and the State: Towards a Strategy for Cyberpower*.

[33] Guterres, "Secretary-General's Address at the Opening Ceremony of the Munich Security Conference"; Khalip, "U.N. Chief Urges Global Rules for Cyber Warfare."

5.4.1 Conceitos Gerais

5.4.1.1 Soberania

A rápida expansão do ciberespaço trouxe consigo uma percepção de liberdade e proximidade espacial nunca experimentadas. É possível quase instantaneamente visitar um museu na França e uma biblioteca na Itália, assistir a um festival popular na Índia, e comprar livros nos EUA ou produtos eletrônicos na China. A Internet, concebida como uma alternativa de comunicação resiliente em caso de ataques nucleares, foi pensada para tornar a comunicação indetectável e, portanto, além do controle ou censura do Estado. O uso de "avatares" (imagens e identidades virtuais) ocultaria a identidade dos usuários, proporcionando uma sensação de anonimato (e impunidade de irregularidades).

> "Os e-libertários um tanto românticos sugeriram que o ciberespaço permitiria que os usuários ficassem longe da distopia do mundo real, que aprisiona e oprime a todos. Parecia oferecer uma quase utopia, o mundo perfeito inatingível"[34].

O ciberespaço estaria totalmente desconectado do mundo real, cujas normas não se aplicariam ali. Quando a administração do presidente Bill Clinton sancionou a Lei de Telecomunicações de 1996, John Perry Barlow reagiu publicando sua icônica Declaração da Independência do Ciberespaço [35]. "Na maioria das vezes, porém, essa noção é um mito. Os Estados podem e controlam o ciberespaço quando lhes convém, muitas vezes com mão pesada"[36].

O conceito de soberania está bem definido no direito internacional desde o Caso Ilha de Palmas, em 1928:

---

[34] Malagutti, "Statecraft within Cyberspace", tradução livre.

[35] Barlow, "A Declaration of the Independence of Cyberspace"; Rid, *Rise of the Machines*.

[36] Finnemore and Hollis, "Constructing Norms for Global Cybersecurity."

"Soberania nas relações entre Estados significa independência. Independência em relação a uma porção do globo é o direito de nela exercer, com exclusão de qualquer outro Estado, as funções de um Estado". [37]. Uma das "funções de um Estado" expressamente manifesta é aquela da aplicação da lei.

> O fato de os regulamentos de Tabukan serem, por disposição expressa, declarados aplicáveis às "ilhas de Nanusa e Meamgy aí incluídas" prova que uma ilha com o nome posterior era conhecida e deliberadamente tratada como pertencente ao Estado vassalo de Tabukan[38].

Por conseguinte, quanto Estados aplicam leis sobre o ciberespaço, eles exerceriam soberania sobre este.

Não obstante, a aplicação do conceito de soberania ao ciberespaço tem diferentes interpretações. Enquanto o Reino Unido desconsidera a natureza da soberania no ciberespaço, a França a definiu claramente, considerando que qualquer ataque a hardware, software ou dados residentes em território francês é um atentado contra sua soberania[39]. A Holanda segue a Regra 4 do Manual de Tallinn: "uma violação da soberania é considerada como ocorrendo se: 1) houver violação da integridade territorial do Estado alvo; e 2) houver interferência ou usurpação de funções inerentemente governamentais de outro estado"[40]. A Austrália defende a soberania sobre os dispositivos de informação e comunicação localizados em seu território e afirma que estes não devem ser usados para violar

---

[37] Huber, "Reports of International Arbitral Awards Island of Palmas Case (Netherlands, USA)."

[38] Huber.

[39] Wright, "Cyber and International Law in the 21st Century"; France-Ministère des Armées, "International Law Applied to Operations in Cyberspace."

[40] Nederlands-MoFA, "Appendix: International Law in Cyberspace."

os direitos e obrigações de outra nação, mesmo para ataques que passem por seu território[41].

> As posições dos EUA são um tanto controversas. Em 2012, o consultor jurídico do Departamento de Estado Harold Koh afirmou que "os estados que realizam atividades no ciberespaço devem levar em consideração a soberania de outros Estados, inclusive fora do contexto de conflito armado". Além disso, as "infraestruturas físicas que suportam a internet e as atividades cibernéticas estão geralmente localizadas em território soberano e sujeitas à jurisdição do Estado territorial". Por outro lado, em 2016, seu sucessor, Brian Egan, disse que "operações cibernéticas remotas envolvendo computadores ou outros dispositivos em rede localizados no território de outro Estado não constituem uma violação *per se* do direito internacional". Além disso, "qualquer regulamentação por um Estado sobre assuntos dentro de seu território, incluindo uso e acesso à Internet, deve cumprir as obrigações aplicáveis a esse Estado sob o direito internacional dos direitos humanos". Dessa forma, o envolvimento em atos de espionagem não é considerado uma violação da soberania.[42]

Schmitt[43] aponta que o Reino Unido "presumivelmente oferecerá um limite relativamente baixo para o que constitui coação [em relação ao ciberespaço], pois deve compensar sua rejeição da soberania como regra primária do direito internacional".

---

[41] Australia-Department of Foreign Affairs and Trade, "Australia's International Cyber Engagement Strategy."

[42] Malagutti, "Famous Cyberattacks in Light Og Countries Positions Regarding Principles of International Law."

[43] Schmitt, "France's Major Statement on International Law and Cyber: An Assessment."

5.4.1.2 Normalização

Outro problema do uso cada vez mais frequente de ciberataques por Estados está na "normalização" de algumas práticas que são contrárias ao costume internacional em relação aos conflitos armados[44]. A literatura está repleta de diferentes nomes de ameaças: vírus, *worms*, botnets, Cavalos de Tróia, malware, "código não autorizado", bombas lógicas e assim por diante. Mas todos eles precisam ser "implantados" (instalados) antecipadamente nas redes de destino. Geralmente, a implantação de malware é feita com semanas (ou mesmo meses) de antecedência para que um ciberataque relevante seja bem-sucedido.

Em junho de 2019, uma crise internacional se desenrolou quando o Irã apreendeu um petroleiro britânico no Golfo Pérsico. A Marinha Real enviou imediatamente um navio de guerra para evitar apreensões subsequentes de navios britânicos, em uma atitude facilmente caracterizada como legítima defesa pelas normas internacionais vigentes. Posteriormente, foi revelado que os EUA realizaram ciberataques que danificaram o banco de dados usado pelos iranianos para realizar as apreensões, embora nenhum navio dos EUA tivesse sido afetado[45]. O próprio hackeamento do banco de dados configura uma ação preventiva. E provavelmente exigia o uso de implantes instalados muito antes.

5.4.1.3 Anonimato & Atribuição

É relativamente fácil atribuir uma operação militar cinética a um determinado país e, em seguida, iniciar um contra-ataque, e havendo poder suficiente, eventualmente, dominar e derrotar o atacante. Embora a atribuição de um

---

[44] Libicki, "Norms and Normalization."

[45] Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say."

ataque nuclear seja imperfeita, apenas alguns estados possuem armas nucleares, seus identificadores isotópicos são relativamente bem conhecidos e atores não-Estatais enfrentam altas barreiras de entrada[46].

No entanto, a atribuição precisa em ciberataques não é fácil[47]. Quanto maior a qualidade exigida, mais demorada e cara ela se torna. À medida que a tecnologia forense melhora, os governos aumentam seus recursos de atribuição, mas as atribuições mais precisas parecem vir de empresas privadas de cibersegurança. Possivelmente porque dessa forma os governos não precisam "queimar" suas fontes de inteligência. No caso da Sony de 2014, as autoridades dos EUA rapidamente atribuíram o ciberataque à Coreia do Norte, com ceticismo generalizado, até que semanas depois um vazamento de imprensa revelou que os EUA tinham acesso às redes norte-coreanas[48].

Um dos problemas da atribuição é que os hackers geralmente protegem suas identidades usando técnicas de disfarce e imitando ferramentas e até mesmo o *modus operandi* de outros hackers, fazendo assim parecer que um grupo ou país diferente tenha perpetrado o ataque, o que comumente é chamado de "bandeira-falsa" (*false flag*)[49]. Ademais, com uma "bandeira falsa" cobrindo a origem real dos ataques, a retaliação pode até ser desencadeada contra um país inocente.

No entanto, a arena internacional é política, e não legal. Assim, a atribuição se torna uma questão de grau de confiança, com cada momento político específico exigindo mais ou

---

[46] Nye, "Can Cyber Warfare Be Deterred?"

[47] Buchanan and Rid, "Attributing Cyber Attacks"; Carr, "Cyber Attacks: Why Retaliating against China Is the Wrong Reaction."

[48] US-White House, "Report on Cyber Deterrence"; Nye, "Can Cyber Warfare Be Deterred?"

[49] Buchanan and Rid, "Attributing Cyber Attacks"; Carr, "Cyber Attacks: Why Retaliating against China Is the Wrong Reaction."

menos evidências. Se o teste *cui bono* (quem se beneficia) apontar para um oponente e houver rumores amplamente considerados confiáveis para apoiar a alegação, então a comunidade internacional provavelmente apoiará a acusação, com danos à reputação do acusado sem a apresentação de evidências concretas[50]. Além disso, nem a teoria nem a prática histórica indicam que uma retaliação deva necessariamente ser aplicada contra o real perpetrador de um ataque[51].

Na ciberdissuasão, como no caso da teoria geral da dissuasão, a atribuição pode ser mais ou menos relevante de acordo com o caso específico do ataque e a situação política momentânea, dando alguma latitude ao dissuadido.

> Embora a atribuição precisa da fonte final de um ciberataque às vezes seja difícil, a determinação não precisa ser hermética. Na medida em que as bandeiras falsas são imperfeitas e os rumores sobre a origem de um ataque são amplamente considerados críveis (embora não sejam legalmente probatórios), danos à reputação e ao poder brando de um invasor podem contribuir para a dissuasão.[52]

5.4.1.4 Cultura

A dissuasão é baseada no cálculo de riscos (custos) e ganhos (benefícios) dos ataques. Esses cálculos são afetados pelas percepções. E essas percepções variam: "diferentes partes de organizações complexas (sejam burocracias privadas ou governos) muitas vezes percebem as mesmas ações (e os custos e benefícios associados) de perspectivas muito diferentes"[53].

---

[50] Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective"; Nye, "The Mouse Click That Roared."

[51] Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm."

[52] Nye, "The Mouse Click That Roared."

[53] Nye, "Deterrence and Dissuasion in Cyberspace."

A "cultura estratégica", "a cultura organizacional, ideológica e política contemporânea de um país que afeta o planejamento da guerra", afeta a maneira como os países "veem ou sentem o ciberespaço". Muitos não o fazem "da mesma forma que os Estados Unidos ou mesmo uns aos outros". Considerando essas diferentes culturas estratégicas, "em oposição a um foco quase exclusivo em seus objetivos políticos rígidos", pode resultar em uma frutífera contenção militar cooperativa no ciberespaço[54].

Normas e tabus podem restringir o comportamento no ciberespaço "impondo custos de reputação que podem prejudicar o poder brando de um ator além do valor obtido com um determinado ataque" [55]. Uma possível abordagem ao controle de armas no ciberespaço seria "desenvolver um tabu não contra tipos de armas, mas contra certos tipos de alvos"[56].

Ataques cibernéticos em cascata na infraestrutura nacional de comunicações durante uma guerra ou em preparação para ela podem afetar o relacionamento entre um governo e seus cidadãos degradar o esforço de guerra do país alvo de maneiras ainda não bem compreendidas [57].

Um custo essencial, muitas vezes não considerado, está relacionado aos valores culturais: as ferramentas de ataque vão contra a cultura institucionalizada de Estados não agressivos. Estados não agressivos provavelmente não terão vontade ou estrutura legal para apoiar o desenvolvimento, aquisição ou implantação de ferramentas de ataque.

---

[54] Austin, "Strategic Culture and Cyberspace: Cyber Militias in Peacetime?"

[55] Nye, "Deterrence and Dissuasion in Cyberspace."

[56] Nye.

[57] Austin, "Strategic Culture and Cyberspace: Cyber Militias in Peacetime?"

5.4.2 Conceitos da "Teoria da Causação"

5.4.2.1 Coação

Clausewitz escreveu que "a guerra é um ato de força para compelir o inimigo a fazer nossa vontade" [58]. "Coação" é um ato de força para compelir o inimigo a fazer nossa vontade, pela ameaça de guerra.

Embora não se espere (pelo menos por enquanto) que ciberataques causem baixas em massa, eles ainda podem ser meios eficazes de coação política em diferentes níveis. Do ponto de vista estratégico, podem ser usados para paralisar infraestruturas críticas, enquanto do ponto de vista tático, podem ser usados para danificar ou incapacitar sistemas militares e de inteligência[59]. Do ponto de vista operacional, a Agência de Logística de Defesa dos EUA estabeleceu que a segurança cibernética constitui um risco significativo que impõe desafios severos às cadeias de suprimentos militares em todos os momentos[60].

Existem vários casos ilustrativos de coação por cibermeios. Ataques do tipo Distributed Denial of Service (DDoS), atribuídos à Rússia, foram realizados contra a Estônia em 2007 e contra a Geórgia em 2008. No caso da Estônia, os ataques iniciaram quando o governo estoniano decidiu mover, da área central de Tallinn para os arredores da cidade, uma estátua representando os soldados soviéticos mortos para libertar a Estônia da dominação nazista. No caso da Geórgia, o sistema de comando e controle de defesa foi bloqueado, e as

---

[58] Clausewitz, *On War*.

[59] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War."

[60] Agency, "Defense Logistics Agency Strategic Plan 2015-2022."

forças militares daquele país não puderam reagir à invasão militar cinética russa de seu território[61].

Em 2010, o malware Stuxnet, que se acredita tenha sido desenvolvido pelos Estados Unidos e Israel, danificou a cascata de centrífugas de enriquecimento de urânio da central nuclear de Natanz, no Irã, alegadamente atrasando em anos o programa nuclear daquele país e coagindo-o a aceitar um acordo de supervisão internacional de aquele programa[62].

Em dezembro de 2015, em meio à crise da região de Dombas, e em pleno inverno europeu, companhias elétricas ucranianas sofreram um ataque cibernético que provocou a interrupção do fornecimento de energia em grande parte daquele país[63].

Uma das dificuldades nas operações de influência no ciberespaço reside em determinar se uma tentativa produziu os resultados desejados[64]. Exceto no caso do Stuxnet, não há indícios de que os outros casos citados tenham resultado nas ações pretendidas.

5.4.2.2 Resiliência

A resiliência, no ciberespaço, consiste em ações que visam aumentar a capacidade de resistir ao avanço do atacante no ciberespaço defendido. Decorre do entendimento da impossibilidade de garantir total efetividade nas ações de

---

[61] Clarke and Knake, *Cyber War: The next Threat to National Security and What to Do about It*.

[62] Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*; TED Talks, *Ralph Langner: Cracking Stuxnet, a 21st-Century Cyber Weapon*; Falliere, Murchu, and Chien, "W32.Stuxnet Dossier."

[63] Dragos, "CRASHOVERRIDE: Analyzing the Threat to Electric Grid Operations"; Zetter, "Everything We Know About Ukraine's Power Plant Hack"; Auchard and Finkle, "Ukraine Utility Cyber Attack Wider than Reported."

[64] Libicki, "Cyberdeterrence and Cyberwar."

proteção. Um dos objetivos centrais da resiliência é manter os sistemas atacados operando, mesmo que degradados. Outra visa a recuperação dos sistemas afetados no menor tempo possível. Muitas vezes esses objetivos entram em conflito entre si, pois a restauração da condição normal do sistema pode implicar na suspensão temporária de sua operação degradada durante o processo de sua restauração[65].

Exemplos de ações para aumentar a resiliência cibernética incluem backups de arquivos clássicos, redundância e replicação de rede e servidor, virtualização de servidores, processamento e balanceamento de carga de rede, monitoramento e restauração de configurações e aplicativos alterados sem a devida autorização e o uso de serviços baseados na "nuvem"[66].

Libicki[67] explicou que quando sistemas são atacados, as vulnerabilidades reveladas são reparadas ou contornadas, tornando tais sistemas mais seguros e resilientes, culminando em uma sociedade mais resistente a futuras tentativas de coação. No entanto, cumpre observar que isso só é verdade se, e quando, o ataque for descoberto.

5.4.2.3 Sinalização

A dissuasão depende das percepções do dissuasor e do dissuadido e da capacidade de comunicarem claramente essas percepções[68]. Os EUA, por exemplo, declararam pretender usar "uma política declaratória e comunicações estratégicas matizadas e graduadas" para destacar seu "compromisso de usar suas capacidades para se defender de ciberataques", mantendo-se "ambíguo quanto aos limites de resposta e consequências para desencorajar preempção ou

[65] Amin Naves and Malagutti, "Defesa Cibernética (Ou Ciberdefesa)."

[66] Amin Naves and Malagutti.

[67] Libicki, "Cyberdeterrence and Cyberwar."

[68] Nye, "Deterrence and Dissuasion in Cyberspace."

ciberatividades maliciosas logo abaixo do limite de resposta"[69]. Essa política declaratória "deixou claro que a dissuasão não se limita ao cibernético contra o cibernético (embora isso seja possível), mas pode ocorrer em outros domínios ou setores com qualquer arma de sua escolha, incluindo nomeação-e-constrangimento (*naming-and-shaming*), sanções econômicas e até armas nucleares"[70].

No âmbito das capacidades convencionais, um clássico desfile militar fornece aos oponentes uma compreensão razoável do poder dos meios ofensivos e defensivos. Considerando o longo ciclo de vida das armas modernas, elas ainda devem apresentar valor dissuasivo continuado por duas ou três décadas. Posicionar esses meios geograficamente fornece alguns indícios sobre "vontade" e "determinação" de aplicá-los. E o comportamento histórico de um Estado provê credibilidade.

No ciberespaço é muito mais complexo. Como meios imateriais, os recursos cibernéticos não podem ser mostrados abertamente. O uso de recursos ofensivos quase certamente os tornará obsoletos em questão de semanas ou meses, no máximo.

> Em contraste, o adversário terá muito menos evidências da extensão e eficácia das capacidades cibernéticas ofensivas dos EUA. Não apenas são totalmente invisíveis, mas podem não ser testados contra sistemas adversários, deixando o adversário com algumas dúvidas sobre a eficácia das capacidades dos EUA e, por sua vez, sobre a credibilidade de suas ameaças. [71]

---

[69] US-White House, "Report on Cyber Deterrence."

[70] Nye, "Deterrence and Dissuasion in Cyberspace."

[71] Farrell and Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine."

Além disso, estabelecer as chamadas "linhas vermelhas", os limites que indicam qual ação indesejada desencadeará uma resposta, também é complicado no ciberespaço. A dificuldade vem da "falta de uma métrica discreta para a ciberguerra", dificultando a avaliação dos efeitos tanto em um primeiro ataque quanto em um de retaliação[72]. Em outras palavras, como consequência direta da natureza de propagação "imprevisível" e "incontrolável" das armas cibernéticas, a avaliação prática dos danos de batalha (BDA) é praticamente impossível[73].

A política de indiciamentos individuais de agentes chineses supostamente responsáveis por ataques cibernéticos, embora seja altamente improvável de resultar em processos bem-sucedidos no sentido de aplicar sanções efetivas aos condenados, sinaliza as prioridades dos EUA e exerce constrangimento público sobre a China [74].

A sinalização, para a ciberdissuasão por punição (ciber-DbP), como para qualquer outro domínio, é essencial e deve ser eficaz, reduzindo os riscos de mal-entendidos ou interpretações errôneas, que podem resultar em um aumento do risco de escalada e conflito. "Isso pode ser feito abertamente, secretamente ou por meio de canais diplomáticos, econômicos ou militares"[75].

Estratégias nacionais, documentos de posicionamento, doutrinas e regras de engajamento também aumentam a credibilidade, podendo servir como "políticas declaratórias", pois declaram intenções que são percebidas por possíveis opositores. Como tais, elas precisam ser verificáveis, o que significa que o comportamento e os recursos aplicados

---

[72] Libicki, "Pulling Punches in Cyberspace."

[73] Malagutti, "State-Sponsored Cyber-Offences."

[74] Farrell and Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine."

[75] Iasiello, "Is Cyber Deterrence an Illusory Course of Action?"

precisam ser consistentes com as declarações. Elas também devem ser robustas sob mudanças, o que significa que devem resistir por algum tempo sem demandarem alterações[76].

> Além da política declaratória, os Estados Unidos também usarão comunicações estratégicas como ferramenta de dissuasão. Em alguns casos, o governo pode destacar investigações, acusações criminais, processos bem-sucedidos ou outras atividades de aplicação da lei que melhorem a postura de dissuasão dos EUA.[77]

Além disso, "sistemas de alerta precoce" que podem detectar e "determinar as intenções do adversário, […] podem ser necessários para exibir capacidades como um meio de sinalizar determinação [ou vontade] para inimigos potenciais e reais"[78].

5.4.2.4 Compelimento, Incentivos e Persuasão

Um dos problemas do debate sobre "deterrência" até agora é um mal-entendido sobre o contexto real da cibercoação. Na maioria dos casos que as nações enfrentam hoje, "a questão mais premente não é dissuadir um ator de optar por realizar intrusões hostis no ciberespaço, mas forçá-lo a parar de realizar intrusões que já foram altamente bem-sucedidas"[79].

Em julho de 2011, o General James Cartwright, do Estado-Maior Conjunto dos EUA, "expressou a esperança de que o Departamento de Defesa mudasse, dentro de uma década, deixando de ser '90% focado na defesa para ser 90%

---

[76] Lukasik, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains."

[77] US-White House, "Report on Cyber Deterrence."

[78] Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace."

[79] Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective."

focado na deterrência'"[80]. Não há dúvida de que a postura dos EUA continuará agressiva. Lembrando que Schelling[81], o principal teórico da Teoria da Coação (ou da Deterrência), observou que a defesa se tornou um eufemismo para a guerra, a interpretação do texto a seguir é bastante ilustrativa.

> Para preservar, bem como aumentar a segurança nacional/interna, é, portanto, importante pensar, desenvolver e sustentar, ao longo do tempo, em um ecossistema em rápida evolução (tecnológica e de segurança/defesa) as capacidades necessárias dos EUA para apoiar o país, com credibilidade e efetivamente, estando pronto e **sendo capaz de dissuadir, deterrer e compelir seus adversários**.[82]

Em 2012, a Diretiva de Política Presidencial 20 (PPD-20) instruiu "os militares a elaborar uma lista de alvos no exterior 'de importância nacional' onde seria mais fácil ou mais eficaz para os Estados Unidos atacar com uma arma cibernética do que uma arma convencional."[83]. "No espectro das hostilidades cibernéticas, os Estados Unidos estão no polo agressivo"[84].

Mais recentemente, as políticas norte-americanas de "Defesa à Frente" (*Defend Forward*) e "Engajamento Persistente" (*Persistent Engagement*) mostraram sua crescente disposição de interferir ofensivamente sempre que

---

[80] Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace."

[81] Schelling, *Arms and Influence: With a New Preface and Afterword*.

[82] Cilluffo, Cardash, and Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strenght."

[83] Harris, *@War*; US-White House, "Presidential Policy Directive/PPD-20."

[84] Harris, *@War*.

considerarem que enfrentam uma ameaça[85]. Na mesma linha, embora um pouco mais contidos, os britânicos desenvolveram seu conceito de Defesa Cibernética Ativa[86].

Incentivos estão frequentemente presentes no desenvolvimento de normas. Estados fortes geralmente oferecem acordos comerciais preferenciais ou acordos de armas, para incentivar os estados mais fracos a apoiar a criação e o cumprimento de normas. Alternativamente, "coação antiquada – sanções econômicas e, no extremo, ações militares ou ameaças críveis – também podem ser empregadas para promover as normas dos fortes"[87].

A persuasão também é comum na negociação de normas internacionais. Pode ser entendido como "fazer alguém fazer ou acreditar em algo perguntando, argumentando ou dando razões", sendo um "processo cognitivo de troca de informações e argumentação que muda mentes, opiniões e atitudes sobre causalidade e efeito na ausência de coação " [88].

Em segundo lugar, quando confrontado com uma situação de compelimento no ciberespaço, o maior desafio da política é identificar os custos apropriados ou a dor a ser infligida ao invasor para fazê-lo mudar seu comportamento da maneira desejada (por exemplo, tirá-lo das redes críticas). Se a política se restringir a ações de retaliação no ciberespaço, as opções do atacado podem ser limitadas[89].

O anonimato proporcionado pelo ciberespaço permite uma estratégia de coação flexível, permitindo que o Estado compelente se comunique e aplique a medida compelente de

---

[85] Smeets, "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection."

[86] Stevens et al., "UK Active Cyber Defence."

[87] Finnemore and Hollis, "Constructing Norms for Global Cybersecurity."

[88] Finnemore and Hollis.

[89] Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective."

forma reservada, enquanto permite que o Estado compelido planeje tranquilamente sua resposta, sem influência de terceiros [90].

5.4.2.5 Capacidades

As capacidades de defesa das potências médias devem ser dimensionadas considerando as ameaças e oportunidades apresentadas pelos países mais poderosos e envolver suas intenções e meios atuais, bem como suas intenções e capacidades futuras mais prováveis [91].

É importante considerar

> o caráter altamente dinâmico do campo político representado pela ciberguerra [ou guerra apoiada pela cibernética] à medida que os países acumulam capacidades, que as opções tecnológicas se expandem e que os principais governos de interesse continuam a se mover decisivamente em direção ao domínio da informação como uma estratégia militar abrangente. [92]

As capacidades devem ser críveis e demonstráveis para que um adversário seja dissuadido pela "detecção e preempção" [93]. As dificuldades em se demonstrar abertamente as capacidades cibernéticas podem fazer com que as ameaças de retaliação cibernética sejam menos críveis do que as de retaliação cinética, porque um estado terá maior dificuldade em demonstrar suas capacidades de empreender ciberataques[94].

---

[90] Hare.

[91] Austin, "Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security."

[92] Austin.

[93] Grimaila, Mills, and Beeker, "Applying Deterrence in Cyberspace."

[94] Farrell and Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine."

A natureza imaterial das capacidades cibernéticas (software) "torna a transparência das capacidades reais difícil, se não impossível" [95] . Além disso, "é difícil conceber demonstrações cibernéticas potencialmente prejudiciais à nação que sejam seguras"[96].

As capacidades cibernéticas devem ser adequadas e específicas para o tipo de dissuasão pretendido. Os recursos de software ofensivos podem servir para Dissuasão por Punição (DbP); se usados em ataques preventivos, que são considerados um movimento defensivo, o que não é um assunto pacificado no Direito Internacional, servem para Dissuasão por Negação (DbD). Ciberarmas defensivas aplicam-se exclusivamente à DbD.

5.4.2.6 Vontade (ou Determinação)

Declarações públicas dos EUA, assim como os casos Stuxnet e Snowden, mostram que os norte-americanos têm vontade e determinação no sentido de empregarem suas capacidades. As políticas *Defend Forward* e *Persistent Engagement* confirmam isso. Da mesma forma, o NCSS britânico e a política de Defesa Cibernética Ativa (*Active Cyber Defence* – ACD) confirmam a determinação do Reino Unido em usar as suas. As declarações públicas da França sobre promoverem interferência quando identificadas ameaças cibernéticas à França sinalizam a mesma postura.

Atribuições feitas pelos EUA, Reino Unido, França, Alemanha, Noruega, Suíça e Estônia, para citar alguns, indicam que China, Rússia, Irã, Coreia do Norte e Canadá empregaram suas cibercapacidades. Ademais, essas atribuições também mostram "determinação" e "vontade". E algumas capacidades.

---

[95] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War."

[96] Lukasik, "A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains."

No entanto, nenhuma atribuição pública significativa foi feita indicando Brasil, Alemanha, Japão, México ou Índia como perpetradores de ciberofensas estatais. Exceto se alguém pretender considerar que a Coreia do Norte tem mais capacidade cibernética do que esses países, a diferença permanece na "vontade/determinação" de empregarem seus cibermeios. Ou, mais precisamente, na falta dela!

Além disso, os EUA, o Reino Unido e a França declararam publicamente seu direito de responder não necessariamente "na mesma moeda" caso um ciberataque cause efeitos significativos nesses países. Assim, eles indicaram que podem usar ataques cinéticos, e mesmo nucleares, para responder a um ciberataque. No entanto, tais ataques continuam a ser relatados. A razão pode ser simples"

> Os deterrentes convencionais e nucleares dos EUA podem ser relativamente ineficazes contra um adversário 'ciberarmado' se o adversário acreditar que os EUA não reagirão a um ataque cibernético com uma resposta entre domínios"[97].

5.4.2.7 Credibilidade

A dissuasão demanda convencer os inimigos em potencial de que os custos da ação hostil excedem os benefícios percebidos. Assim, desenvolver e sinalizar capacidades reforçará a credibilidade[98].

Capacidades e credibilidade devem ser calibradas de acordo com os objetivos políticos pretendidos. Os investimentos e esforços devem refletir a proporção desejada de ataque e defesa, e a recalibração permanente deve ser cuidadosamente considerada e ajustada conforme necessário[99].

---

[97] Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War."

[98] Cilluffo, Cardash, and Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strenght."

[99] Cilluffo, Cardash, and Salmoiraghi.

Na DbP, as ameaças devem ser dimensionadas de acordo com o tamanho do objetivo. Uma ameaça excessivamente grande geralmente não é crível, e as menores podem fornecer um efeito mais dissuasivo[100]. No caso dos EUA, não há falta de credibilidade em suas capacidades ou em sua vontade[101]. Além disso, como sua postura e cultura são agressivas, focadas em DbP, suas ameaças devem causar efeito. Uma possível razão pela qual não é pode ser o efeito limitado esperado em ciberataques.

Um ataque de retaliação também pode não ter sido percebido, ter falhado ou ter sido atribuído incorretamente[102]. Também pode ter sido considerado um erro operacional, ou até mesmo ter sido deliberadamente ignorado.

Boas defesas aumentam a credibilidade. Elas reduzem a probabilidade de um ataque ser bem-sucedido, reduzindo assim o número de potenciais desafiantes, ao mesmo tempo em que facilitam a atribuição[103].

A ausência ou a qualidade de regras de engajamento e doutrinas também podem afetar a credibilidade[104]. Na falta de exemplos anteriores (ou históricos) de comportamento, elementos subsidiários como estratégias nacionais, *white papers* e *green papers*, *position papers*, doutrinas e regras de engajamento podem subsidiar a criação de uma percepção de maturidade e capacidade, aumentando a credibilidade.

Parcerias público-privadas (PPP) robustas também aumentam a credibilidade, pois podem "promover as melhores práticas de cibersegurança; auxiliar na construção da confiança do público nas medidas de cibersegurança; e dar credibilidade

---

[100] Farrell and Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine."

[101] Farrell and Glaser.

[102] Libicki, "Cyberdeterrence and Cyberwar."

[103] Libicki.

[104] Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace."

aos esforços nacionais para aumentar a resiliência da rede"[105]. Também podem estimular o surgimento ou fortalecer fornecedores nacionais de produtos e serviços de cibersegurança.

5.5 Ciberdissuasão na Doutrina Brasileira

A falta de um *corpus* adequado sobre deterrência e dissuasão no Brasil mostra uma visão limitada particularmente relevante no que diz respeito à ciberdefesa e cibersegurança. Recordemos a definição de dissuasão presente na Estratégia Nacional de Defesa do Brasil:

> DISSUASÃO - Atitude estratégica que, por intermédio de **meios de qualquer natureza, inclusive militares**, tem por finalidade desaconselhar ou desviar adversários, reais ou potenciais, de possíveis ou presumidos **propósitos bélicos**. O mesmo que DETERRÊNCIA.[106]

Diversas nações elaboram estratégias de ciberdefesa e cibersegurança visando deterrer ações de fins não militares, como espionagem comercial, industrial e política, terrorismo, ameaças de interrupção da operação de infraestruturas críticas ou estratégicas e outras formas de defesa cibernética estatal. No entanto, pela definição adotada, o Brasil estaria sinalizando não pretender agir de forma dissuasória nessas situações, haja vista que "não bélicas".

Na mesma linha, temos a determinação referente aos "projetos estratégicos", "indutores do processo de transformação" do Exército Brasileiro, cuja continuidade é necessária para alcançar o "grau de dissuasão desejado", dentre os quais o Sistema de Defesa Cibernética, que atuam aumentando a mobilidade, a atividade de vigilância e controle

---

[105] US-White House, "Report on Cyber Deterrence."

[106] Brasil-MD, "Política Nacional de Defesa e Estratégia Nacional de Defesa", grifos nossos.

de fronteiras e a capacidade de atuar na negação de acessos indesejados a áreas ou sistemas estratégicos de interesse da Defesa Nacional[107]. Claramente, a Estratégia Nacional de Defesa brasileira é baseada numa abordagem de dissuasão por negação (incluindo a ciberdefesa). Mas a implementação carece de sustentação para os elementos teóricos fundamentais da Teoria da Dissuasão.

5.6 Conclusão

Neste capítulo buscou-se conceituar a que seria a ciberdissuasão e sua importância para a proteção da segurança nacional no ciberespaço, e mesmo fora dele.

Para tal, foi inicialmente discutida a necessidade da ciberdissuasão como um tópico crescente de pesquisa, associada ao crescimento da importância dos computadores nas economias e sociedades modernas. Foi também apresentada a correlação entre a segurança nacional e o ciberespaço. Em seguida foi discutida a aplicação dos conceitos de dissuasão (entendida como mais que a "simples" deterrência) ao ciberespaço, e analisada a possibilidade de uso do quinto domínio da guerra como um instrumento de coação ou coação.

Por fim, analisou-se a ciberdissuasão na doutrina brasileira, constatando-se que, se já havia pouca profundidade teórica no tocante à dissuasão clássica, há menos ainda no tocante à ciberdissuasão, sendo necessário o aprofundamento do tema antes que se amplie o distanciamento do Brasil com os países do "arco do conhecimento" no ciberespaço.

[107] Brasil-MD.

6 Os Seis Tipos de Ciberdissuasão

Este capítulo analisa a aplicação, ao ciberespaço, dos diferentes tipos de dissuasão identificados em *Dissuasão: Um Olhar Brasileiro*[1]. Seus elementos constitutivos são estudados à luz das diferentes visões que permeiam o debate atual no ambiente acadêmico internacional, considerando as dificuldades técnicas, políticas e econômicas de implementação cada uma dessas formas de ciberdissuasão.

6.1 Introdução

O corpus de conhecimento sobre dissuasão gerado desde a proposta inicial de Kauffman[2], em 1954, aponta para a existência de seis tipos de dissuasão[3]:

- Punição (*Dissuasion by Punishment* – DbP);
- Negação (*Dissuasion by Denial* – DbD);
- Futilidade (*Dissuasion by Futility* – DbF);
- Normas (*Dissuasion by Norms* – DbN);
- Emaranhamento (*Dissuasion by Entanglement* – DbE); e
- Individualização (Dissuasion by Individualisation – DbI).

Neste capítulo discute-se a adaptação dos preceitos fundamentais de cada um desses ao ciberespaço.

6.2 Punição

Ciberdissuasão por Punição (C-DbP) depende da capacidade de projetar poder no ciberespaço do oponente. Os objetivos táticos da C-DbP, derivados do conceito geral de

[1] Malagutti, *Dissuasão: Um Olhar Brasileiro*.

[2] Kaufmann, "The Requirements of Deterrence."

[3] Malagutti, *Dissuasão: Um Olhar Brasileiro*, Capítulo 5.

DbP, podem ser "interromper um ciberataque enquanto ele está acontecendo, punir os infratores depois que ele aconteceu ou punir os infratores antes que eles lancem um ataque inicial" [4] . Isso, claro, se o país entender que ataques preemptivos ou preventivos são legalmente, moralmente e "culturalmente" aceitáveis.

A DbP depende da existência de "reféns de contravalor", alvos ameaçáveis valorizados pelo atacante, não necessariamente militares. "Alvos valiosos incluem o povo de um Estado, possivelmente sua liderança, sua economia, e afins, a infraestrutura que suporta o povo daquele Estado e sua economia"[5].

Uma questão importante relacionada à resposta a ciberataques diz respeito à "proporcionalidade". Uma resposta, para ser legalmente válida, deve causar efeitos semelhantes àqueles produzidos pelo ataque do agressor. No entanto, dependendo do nível de desenvolvimento técnico, social e econômico de um país, ele oferece diferentes "superfícies de ataque" para ciberataques. Uma "'resposta na mesma moeda' pode ter implicações totalmente diferentes para os Estados Unidos e para o agressor"[6].

Além disso, considerar ciberataques retaliatórios apresenta riscos de escalada, uma vez que "a capacidade de conduzir um ataque orquestrado com resultados previsíveis e controláveis é considerada mais uma opção em desenvolvimento do que uma capacidade atual"[7].

Em 1995, a única resposta punitiva disponível para a Rússia contra ciberataques era uma resposta nuclear; isso foi baseado na crença de que "mesmo quando as defesas são ruins,

---

[4] Iasiello, "Is Cyber Deterrence an Illusory Course of Action?"

[5] Farrell and Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine."

[6] Kissinger, *World Order*.

[7] Elliott, "Deterring Strategic Cyberattack."

uma capacidade de retaliação devastadora pode impedir que os ataques sejam preparados em primeiro lugar" [8]. Da mesma forma, em 2011, esperava-se que uma política semelhante "emergisse de esforços futuros para esfriar o ardor dos entusiastas da ciberguerra, como na nova política dos EUA de ameaçar responder a ciberataques com meios militares convencionais"[9].

> Se o ciberataque do adversário tivesse destruído parte da rede elétrica dos EUA, refinarias de petróleo e ou oleodutos, os EUA poderiam retaliar esses alvos de infraestrutura na terra natal do invasor. Alternativamente, os EUA poderiam optar por ameaçar um tipo de dano bem diferente daquele infligido pelo ciberataque. Por exemplo, exceto diante de uma grande potência, os EUA poderim ameaçar invadir o país do atacante ou impor um novo regime, se o país lançar um ciberataque de contravalor extremamente destrutivo contra os EUA. Esses custos seriam muito diferentes daqueles impostos pelo ciberataque do adversário, mas os custos não precisam ser de tipos semelhantes para que um adversário seja dissuadido. Em termos de abordagem baseada em efeitos básicos, a principal consideração para os Estados Unidos não deve ser se se deve responder na mesma moeda – seja em termos de meios ou alvos – mas sim qual ameaça de resposta provavelmente será mais eficaz.[10]

As políticas que ameaçavam uma resposta dos EUA não "na mesma moeda" foram de fato comunicadas, mas não

---

[8] Arquilla, "From Blitzkrieg to Bitskrieg: The Military Encounter with Computers."

[9] Arquilla.

[10] Farrell and Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine."

resultaram em dissuasão efetiva, pelo menos se considerados os frequentes anúncios e atribuições de ciberataques.

As dificuldades na atribuição de ciberataques e intrusões são frequentemente relatadas como um problema que prejudica o C-DbP: "como podemos responder de forma eficaz se não sabemos quem fez o quê?"[11]. No entanto, como já observado, a atribuição tem um forte componente político.

O suporte de credibilidade e recursos para C-DbP incorre em altos custos, e esses custos são recorrentes devido ao curto ciclo de vida das ciberarmas.

> Até o momento, os custos assumidos para sinalizar credibilidade para a dissuasão por ameaças de punição no ciberespaço para os Estados Unidos incluem o desenvolvimento de 133 equipes de missões nacionais cibernéticas, a provisão de bilhões de dólares em investimentos para manter o Comando Cibernético dos Estados Unidos e a criação de filiais de forças cibernéticas no Exército, Marinha, Força Aérea e Corpo de Fuzileiros Navais. A NSA e a CIA também continuaram o desenvolvimento de cibercapacidades. É razoável crer que cada uma dessas organizações esteja desenvolvendo uma variedade de explorações, definidas na Doutrina de Operações do Ciberespaço JP 3–12 como cibercapacidades. No entanto, ao contrário dos domínios físicos de terra, mar, ar e espaço, a vida útil das capacidades desenvolvidas é limitada temporalmente tanto pelas mudanças na tecnologia decorrente da evolução das plataformas de software e hardware, pela manutenção das plataformas existentes e pela frequência com que essas

[11] Grimaila, Mills, and Beeker, "Applying Deterrence in Cyberspace"; Buchanan and Rid, "Attributing Cyber Attacks"; Finnemore and Hollis, "Constructing Norms for Global Cybersecurity."

> plataformas estão conectadas ou podem ser acessadas pela Internet. [12]

Para poder retaliar na mesma moeda, as ferramentas de ciberataque dependem de planejamento e preparação cuidadosos. Elas precisam ser implantadas previamente nas redes visadas, exigindo a necessidade de meios para manter, atualizar e acionar os implantes para realizar um ataque abrangente e eficaz. Isso pode ser complicado. O oponente pode encontrar esses implantes antes do ataque ser realizado e neutralizá-los antes de serem usados. Nesse caso, o dissuasor pensaria que suas ciberarmas ainda estão disponíveis e contaria com elas e, quando necessárias, elas não mais seriam eficazes. Alternativamente, o próprio implante poderia ser considerado o prelúdio do ataque, desencadeando um ataque preventivo por parte do dissuadido, não necessariamente "na mesma moeda"[13].

A punição também requer um nível um tanto elevado de atribuição. Ademais,

> quando uma vítima de um ataque anônimo divulga publicamente o código do malware invasor para que os *patches* possam torná-lo inútil, isso tem um custo elevado para o atacante, principalmente se houver explorações caras de dia zero (falhas de software anteriormente desconhecidas)[14].

6.3 Negação

A Ciberdissuasão por Negação (C-DbD) depende de capacidades defensivas para implementar a negação de área no ciberespaço do dissuasor para atividades indesejadas. Embora Snyder tenha definido a defesa como a soma de dissuasão e

---

[12] Brantly, "Entanglement in Cyberspace: Minding the Deterrence Gap."

[13] Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*.

[14] Nye, "Deterrence and Dissuasion in Cyberspace."

resiliência, a literatura contemporânea considera a resiliência uma parte da dissuasão por negação. Assim, o C-DbD conta com capacidades de ciberdefesa (chamadas de proteção cibernética na doutrina brasileira) e de ciberresiliência[15].

Embora sempre haja atores sofisticados capazes de frustrar as defesas de cibersegurança mais robustas, na maioria das vezes o sucesso da atividade hostil contra as redes é resultado de práticas de cibersegurança ruins[16].

A defesa (ou proteção) inclui medidas para neutralizar ações ofensivas e exploratórias do atacante contra os sistemas do defensor. É materializada pelo estabelecimento de camadas sobrepostas que oferecem diferentes tipos e níveis de resistência a intrusões nos sistemas protegidos. A sobreposição dessas camadas protetoras aumentará a eficácia das camadas protetoras[17].

Exemplificando, as medidas de proteção compreendem mecanismos e as "melhores práticas" do ciberespaço: o uso de métodos robustos de autenticação (identificação) e autorização (restrição de privilégios) de usuários, a segregação de redes, o uso de listas de acesso, o uso de sistemas de prevenção de intrusão e ferramentas antivírus, a adoção de criptografia em informações confidenciais (não apenas em trânsito, mas também quando armazenadas estaticamente), o uso de firewalls, ouso de redes virtuais privadas (VPN), o monitoramento de tráfego de rede, a busca por protocolos e endereços de rede espúrios ou volumes anormais de tráfego e a instalação regular de atualizações (*patches*) de segurança[18].

Também é imperativo estabelecer um sistema abrangente, ágil e eficaz de centros de prevenção e tratamento de ciberincidentes (CSIRTs). A cooperação entre esses

[15] Malagutti, "Why Should Nations Pursue Their Software Power ?"

[16] Iasiello, "Is Cyber Deterrence an Illusory Course of Action?"

[17] Amin Naves and Malagutti, "Ciberdefesa (Ou Ciberdefesa)."

[18] Amin Naves and Malagutti.

centros, nacional e internacionalmente, muitas vezes ajuda a identificar, conter e neutralizar ciberofensas. Além disso, permite a coleta de dados que suportam ações investigativas, antes que possam ser comprometidas por ações de resiliência[19].

No geral, a C-DbD é uma atividade cotidiana no ciberespaço, praticada por meio de ferramentas e procedimentos de cibersegurança bastante conhecidos[20].

A natureza custosa de boas defesas é geralmente o primeiro e mais significativo desafio citado para C-DbD. Para cada classe de ação existe um tipo diferente de ferramenta defensiva[21]. Analisando o espectro de atividades e ferramentas necessárias para a implementação das medidas mencionadas, é fácil concluir que os custos de aquisição, instalação, configuração, operação e suporte de todos os itens, multiplicados pelo número de redes, computadores e usuários nas sociedades modernas, são altos[22].

O segundo desafio histórico diz respeito à percepção comum de que os sistemas devem ser defendidos em suas fronteiras, suas interfaces externas. Essa abordagem da Linha Maginot certamente falhará, pois *firewalls* e IDSs detectam apenas o que já conhecem e deixam escapar novas ameaças[23]. Algumas intrusões escaparão da detecção nas fronteiras dos sistemas, e os defensores devem ser capazes de caçar intrusos assim que estiverem dentro do perímetro[24].

---

[19] Amin Naves and Malagutti.

[20] Denning, “Rethinking the Cyber Domain and Deterrence.”

[21] Hutchins, Amin, and Cloppert, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.”

[22] Malagutti, “Why Should Nations Pursue Their Software Power ?”

[23] Arquilla, “From Blitzkrieg to Bitskrieg: The Military Encounter with Computers.”

[24] Lynn, “Defending a New Domain: The Pentagon’s Cyberstrategy.”

Resiliência, por conseguinte, deve ser considerada como um elemento fundamental da C-DbD. A adequada preparação "para operar sob coação" envia um forte sinal dissuasório aos potenciais adversários, indicando que o país pretende negar benefícios derivados de ciberataques[25].

> A Agência de Segurança Nacional foi pioneira em sistemas que, usando avisos fornecidos pelos recursos de inteligência dos EUA, implantam automaticamente defesas para combater invasões em tempo real. Parte sensores, parte sentinelas, parte atiradores de elite, esses sistemas de defesa ativos representam uma mudança fundamental na abordagem dos EUA à defesa de rede. Eles trabalham colocando a tecnologia de varredura na interface das redes militares e da Internet aberta para detectar e interromper o código malicioso antes que ele passe para as redes militares. As defesas ativas agora protegem todas as redes de defesa e inteligência no formato ". mil".[26]

A "defesa em profundidade", no entanto, não é uma tarefa fácil. Mais de 600 avaliações descartaram a velha crença na segurança de sistemas "air-gapped" (fechados em redes isoladas); "o tempo médio de detecção de uma invasão de malware é de quatro meses e eles normalmente são identificados por terceiros"; as ameaças evoluem mais rápido que as contramedidas e muito mais rápido do que as políticas; e a demanda por ciberdefensores treinados com conhecimento de sistemas de controle excede amplamente a oferta[27].

---

[25] Beeker et al., "Operationally Responsive Cyberspace: A Critical Piece in the Strategic Deterrence Equation."

[26] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy."

[27] Austin, "Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security."

O terceiro desafio frequentemente citado da C-DbD é que ela precisa incluir o setor privado. A expressão econômica do poder nacional está diretamente ligada àquela militar. Espionagem industrial e atos isolados de sabotagem deixados de lado, historicamente, existiam apenas duas maneiras de se atingir militarmente a economia e a infraestrutura civil de um país. Indiretamente, por meio de bloqueios, ou diretamente, por meio de bombardeios. O poder militar superior do defensor inibiria ambos os casos. As ciberarmas mudaram esse paradigma. O Software Power possibilitou evitar o confronto com forças militares superiores ao viabilizar a cibersabotagem, às vezes chamada de "cibotagem" (*cybotage*) na projeção de poder contra o setor privado, que nas sociedades modernas engloba grande parte da infraestrutura civil[28].

Assim, as ciberdefesas nacionais exigem o compromisso do governo não apenas para proteger suas próprias redes, mas também para cooperar com os proprietários de infraestrutura privada (ou concessionárias)[29]. Tal cooperação seria onerosa e certamente fora do âmbito da atividade empresarial regular das empresas[30]. Por conseguinte, exige novos mecanismos de parcerias público-privadas.

Contra ciberataques patrocinados por Estados, os defensores de empresas privadas devem presumir que suas redes serão, em algum momento, invadidas.

> Se agências de inteligência estrangeiras experientes e bem financiadas estão interessadas em hackear um negócio, é uma boa aposta que pelo menos parte do tempo elas terão sucesso[31].

---

[28] Malagutti, "Why Should Nations Pursue Their Software Power ?"

[29] Iasiello, "Are Cyber Weapons Effective Military Tools?"

[30] Elliott, "Deterring Strategic Cyberattack."

[31] Buchanan, "Corporate Cybersecurity Is Becoming Geopolitical. Are U.S. Tech Companies Ready?"

A forma como se prepararão para conviverem com essa realidade fará a diferença.

Além disso, empresas privadas de cibersegurança e outras empresas de software podem se tornar parceiras do governo na criação de mecanismos de defesa, como já acontece nos EUA. A Microsoft e outras empresas de tecnologia da computação desenvolvem estratégias sofisticadas para detectar códigos maliciosos (como a *backdoor* da Juniper Networks) e impedir sua implantação em suas cadeias de suprimentos globais [32]. Ainda assim, as investigações de um ciberataque recente contra a FireEye, uma renomada empresa de cibersegurança, revelaram uma violação na cadeia de fornecimento de software SolarWind, permitindo que hackers acessassem o Departamento do Tesouro dos EUA e a Administração Nacional de Telecomunicações e Informações (NTIA) do Departamento de Comércio dos EUA, bem como muitas empresas privadas como a própria Microsoft[33].

Não obstante, empresas privadas podem ajudar em muitos tipos de ciberdissuasão. Alguns bons exemplos são:

> os esforços de atribuição de empresas de segurança privada em relação à punição, as ações de empresas multinacionais em enredamento ou as ações empresariais de organizações internacionais e transnacionais na criação e aplicação de normas[34].

No geral, o objetivo da C-DbD não é manter os invasores fora do ciberespaço do defensor, mas "subir a barra"

---

[32] Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy."

[33] Cimpanu, "Microsoft, FireEye Confirm SolarWinds Supply Chain Attack."

[34] Nye, "Deterrence and Dissuasion in Cyberspace."

de custos para tornar mais difícil para eles obter os ativos que buscam[35].

> Independentemente da medida coercitiva adotada, defesas mais fortes e maior resiliência da infraestrutura crítica devem fazer parte de qualquer estratégia para aumentar os custos da condução de ações hostis no ciberespaço[36].

Assim, a negação oferece o melhor meio de dissuasão, seja no ciberespaço ou não, nas situações em que pode ser aplicada e tem boa relação custo-benefício[37].

C-DbD é difícil, embora possível; e é uma resposta primária a ciberataques[38]. E, embora cara, é muito menos cara do que os custos de não se fazer nada, como mostram os números recentes sobre os danos causados por ciberataques.

Kopp [39] listou formas de dissuasão existentes na biologia. Analogias com elas podem fornecer mecanismos de C-DbD interessantes. A primeira forma é a que ele chamou de Degradação (ou também Negação de Informação). Refere-se à "ocultação e camuflagem, ou furtividade", basicamente destinada a ocultar o sinal em meio a ruído suficiente, para que o atacante não tenha certeza do quê significa o quê. No ciberespaço, um paralelo pode ser uma "inundação de informações" com centenas de arquivos (ou servidores virtuais) com nomes e conteúdo semelhantes, dificultando a identificação daquele verdadeiro. A segunda forma Kopp denominou Corrupção (ou Engodo ou Mimetismo),

---

[35] Carr, "Cyber Attacks: Why Retaliating against China Is the Wrong Reaction."

[36] Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective."

[37] Denning, "Rethinking the Cyber Domain and Deterrence."

[38] Elliott, "Deterring Strategic Cyberattack."

[39] Kopp, "The Four Strategies of Information Warfare and Their Applications."

significando "a inserção de informações intencionalmente enganosas, tornando o receptor incapaz de "distinguir o sinal enganoso do sinal real". O uso de "potes de mel" (*honeypots*[40]) no ciberespaço corresponde a esta técnica. A terceira foi denominada Subversão, o que equivaleria a municiar um arquivo para que, quando o invasor o acessasse, o malware nele embutido desencadeasse um processo destrutivo no sistema do atacante.

Os custos das falhas na manutenção da ciber-higiene costumam ser mais altos para um país do que os custos para indivíduos e empresas privadas[41]. Além disso, enquanto um problema para C-DbP, as dificuldades de atribuição favorecem C-DbD[42].

Já foi dito que C-DbD, embora imperfeita, pode ser melhor do que nenhuma dissuasão, e "somente por essa razão, talvez, […] tende a se tornar uma opção padrão, tanto em suas formas pré-evento (defesa) quanto pós-evento (resiliência, gerenciamento de consequências, "absorção de risco")[43]. De fato, pode ser a melhor opção, mas não só por isso, como será demonstrado mais adiante.

6.4 Futilidade

A Ciber Dissuasão por Futilidade (C-DbF) consistiria em tentar convencer uma nação de que não adianta investir em cibercapacidades porque nunca seria possível obter uma vantagem competitiva contra os meios das superpotências. O problema desse conceito é que ele considera quase que

---

[40] *Honeypots* são sistemas construídos deliberadamente, geralmente com vulnerabilidades conhecidas abertas, para se tornarem atraentes para os oponentes e fornecer informações enganosas (contrainteligência), permitindo rastrear e identificar o invasor Kaspersky Labs, "O Que é Um Honeypot? Como Os Honeypots Ajudam a Segurança.".

[41] Nye, "Deterrence and Dissuasion in Cyberspace."

[42] Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace."

[43] Stevens.

exclusivamente uma perspectiva ofensiva, focando na busca de "uma vantagem competitiva".

Os Estados-nação devem considerar a formulação sempre válida de Vegetius: *Si vis pacem para bellum*[44] (se quereis a paz preparai-vos para a guerra)[45]. Nenhum país pode decidir deixar de investir em capacidades defensivas porque considera que nunca terá capacidades ofensivas decisivas.

Capacidades defensivas importam. Nas palavras de Schelling:

> À força, um país pode repelir e expulsar, penetrar e ocupar, apreender, exterminar, desarmar e desabilitar, confinar, negar acesso e frustrar diretamente uma intrusão ou ataque. Pode, isto é, se tiver força suficiente. "Suficiente" depende de quanto o oponente tem.[46]

Além disso, quando já existe um conflito, mesmo capacidades inferiores podem criar algum desconforto em países mais poderosos, como as cibercapacidades iranianas e norte-coreanas usadas contra os EUA mostraram até agora. Outro fator que joga contra o C-DbF é o custo relativamente baixo das cibercapacidades ofensivas em comparação com outras capacidades militares.

> A ciberguerra operacional tem o potencial de contribuir para a guerra – o quanto é desconhecido e, em grande parte, não conhecível. Como um ciberataque devastador pode facilitar ou amplificar as operações físicas, e porque uma capacidade operacional de ciberguerra é relativamente barata, vale a pena desenvolvê-la. Dito isso, o sucesso na ciberguerra não é apenas uma questão de

---

[44] A frase, de fato, é "*qui desiderat pacem, praeparet bellum*". No entanto, tornou-se mais conhecida pela variante usada acima.

[45] Vegetius, *De Re Militari*, book III, Prologus.

[46] Schelling, *Arms and Influence: With a New Preface and Afterword*.

> técnica, mas também requer a compreensão das redes do adversário no sentido técnico e, mais ainda, no sentido operacional (como os adversários potenciais usam as informações para travar a guerra).[47]

No entanto, tudo considerado, a assimetria das cibercapacidades pode de fato exercer algum efeito dissuasório, principalmente por "filtrar" o número de aventureiros em potencial, mas não contra oponentes declarados.

6.5 Normas

Ciber-Dissuasão por Normas (C-DbN) é a variante de DbN para o ciberespaço. É a primeira linhagem de dissuasão nascida após o renascimento da deterrência e da dissuasão como área de estudo devido ao crescimento das ciberameaças.

Até 2017, as normas há muito eram consideradas um elemento coadjuvante das estratégias de dissuasão. No entanto, a abordagem muitas vezes foi a da "ameaça de retaliação" pelo descumprimento das normas estabelecidas[48].

Stevens[49], em *Deterrence and Norms in Cyberspace*, observou que tanto Lewis[50] quanto Nye[51] consideraram que normas poderiam reforçar a dissuasão de cibercrimes, conquanto nenhum deles houvesse "categorizado explicitamente normas como uma forma de dissuasão". Stevens também observou que a Estratégia Internacional dos EUA para o Ciberespaço, de 2011, indicou explicitamente "o surgimento de uma ciberestratégia nacional na qual a ciberdissuasão pode ser buscada não apenas por meio de

[47] Libicki, "Cyberdeterrence and Cyberwar," xx.

[48] Freedman, *Deterrence*.

[49] Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace."

[50] Lewis, "Cross-Domain Deterrence and Credible Threats."

[51] Nye, "Cyber Power."

capacidades de segurança nacional, mas também por meios diplomáticos, informativos, econômicos e políticos"[52].

Em 2015, focado na ciberdissuasão, Davis afirmou:

> Outras formas de influência, incluindo leis e normas sociais e internacionais, também têm um potencial considerável para reduzir alguns tipos de ciberataques. Atitudes e normas provavelmente têm mais potencial do que as leis em si, mas podem se reforçar mutuamente.[53]

Então, em 2017, Nye finalmente nomeou "Dissuasão por Normas" as tentativas normativas de regular o comportamento cibernético[54].

O entendimento popular de normas geralmente está relacionado à existência de um acordo formal ou lei. No entanto, normas podem ser "institucionalizadas", formais ou informais, como leis internas, tradições culturais, morais ou religiosas, ritos, tabus e até mitos, e afetam o comportamento.

Normas são muitas vezes consideradas como relacionadas à Teoria Construtivista das Relações Internacionais (RI)[55]. Além disso, a abordagem construtivista é indiscutivelmente "predominante na literatura comum ao ciber e RI" e "a visão construtivista tende a se concentrar em como o ciberespaço auxilia na ampliação da definição e transformação de ideais, o que contribui para mudanças no status quo social"[56].

No entanto, as abordagens usuais no desenvolvimento de normas consideram a visão realista, centrada no poder. Os tratados requerem o consentimento expresso dos Estados. Gary Corn, ex-assessor jurídico da USCyberCom, observa que

---

[52] Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace."

[53] Davis, "Deterrence, Influence, Cyber Attack and Cyberwar."

[54] Nye, "Deterrence and Dissuasion in Cyberspace."

[55] Freedman, *Deterrence*.

[56] Medeiros and Goldoni, "The Fundamental Conceptual Trinity of Cyberspace."

o princípio básico de qualquer negociação é que "ninguém negocia contra si mesmo"[57]. Na medida em que possuem capacidades que são estrategicamente ou operacionalmente úteis, alguns Estados não têm incentivo para limitar a opção de usá-las[58]. Esses mesmos países, no entanto, também são vulneráveis a operações hostis perpetradas por estados com capacidades semelhantes ou até inferiores. Portanto, diferentes órgãos de um mesmo país veem os interesses nacionais com diferentes perspectivas e podem diferir em como percebem que aquele país deva caracterizar uma determinada prática[59]. Apesar disso, enquanto a lógica aponta para uma vantagem líquida dos prós frente aos contras, prevalece a defesa da manutenção da vantagem estratégica. Libicki afirma que "a regra mais ampla se aplica: as normas estabelecidas em negociações de estado com estado exigem que os proponentes desistam de algo assim como recebam algo para que tais normas persistam" e que "como regra, os países concordam com acordos assimétricos apenas sob coação. Na era Obama, a ameaça eram as sanções"[60]. Entretanto,

> Os poderes coativos – subornos e ameaças – levantam questões importantes não apenas sobre os processos normativos, mas sobre a natureza da própria normatividade. Algo "conta" como norma se o comportamento desejado for coagido (ou subornado) em vez de ser sinceramente acreditado ou aceito? Uma norma é realmente uma norma se não gostarmos de seu conteúdo?[61]

Nye indica duas características diferentes de normas. Uma diz respeito à óbvia oportunidade de retaliação, como se

---

[57] Daskal et al., "Data and Sovereignty."

[58] Mačák, "Is the International Law of Cyber Security in Crisis?"

[59] Schmitt and Vihul, "The Nature of International Law Cyber Norms."

[60] Libicki, "Norms and Normalization."

[61] Finnemore and Hollis, "Constructing Norms for Global Cybersecurity."

depreende da afirmação de que "é necessário algum grau de atribuição para que as normas funcionem"[62]. A outra ele expressa em termos relacionados à ideia de cultura e valores, embora ainda com uma abordagem realista: "um *agressor incipiente* pode ser inibido por sua própria consciência, ou, mais provavelmente, pela perspectiva de perder a posição moral e, portanto, política, permanentemente, com países não comprometidos"[63]. Não obstante, não parece plausível considerar que apenas "agressores incipientes" seriam inibidos pela consciência ou posturas morais e políticas. O general Michael Hayden, ex-comandante do USCyberCom e diretor da NSA, afirmou que:

> A liderança sênior da NSA e do GCHQ se reúne anualmente, alternando qual lado do Atlântico sedia. [...]
>
> [O] GCHQ estava tendo seus próprios problemas com o crescente "europeísmo" da Grã-Bretanha. A sobreposição da Convenção Europeia de Direitos Humanos à lei, à política e à prática britânicas era uma questão importante para o governo. Para o GCHQ, isso significava encargos administrativos e procedimentos adicionais para poder demonstrar sua conformidade.
>
> [...], no final das contas, nós, americanos, passamos bastante tempo nos explicando. Como explicar nossos pontos de vista sobre o uso da força nas relações internacionais. As diferenças eram mais gritantes com muitos europeus continentais, é claro, mas estávamos representando um governo e (eu acho) um povo com, digamos, uma visão mais robusta

[62] Nye, "Deterrence and Dissuasion in Cyberspace."

[63] Nye.

> da utilidade da força do que nossos primos britânicos.[64]

Conforme exposto, a visão do governo americano sobre o uso da força é diferente da dos britânicos, e mais ainda daquela de outros aliados europeus dos EUA (e possivelmente a do povo americano também). E isso não significa que todos esses sejam "agressores incipientes".

Discutindo a ética das ciberoperações ofensivas em um livro dedicado a "projetar os valores do Reino Unido no exterior", Devanny afirma que o que ele chama de ciberescaramuças (*cyber-skirmishing*), operações destinadas a prevenir um ataque, impedir uma campanha de *ransomware* ou punir um ator estatal hostil, e ciberoperações durante conflitos armados, apoiando operações integradas são "mais atraentes". No entanto, as operações destinadas a "sinalização dissuasiva de recursos para minar a infraestrutura crítica, são ética e legalmente mais complexas, para não dizer nada sobre sua eficácia estratégica"[65].

É fundamental notar que a legalidade dos ataques preventivos, assumida por Devanny, não é consensual no cenário internacional. Internacionalistas brasileiros influentes, por exemplo, não reconhecem sua legalidade. Argumentam que, embora o princípio da legítima defesa tenha previsão legal de natureza consuetudinária, não há amparo legal para ações preventivas[66]. A Doutrina Bush, publicada um ano após os ataques terroristas de 11 de setembro, reiterou que os EUA há muito insistem na possibilidade de ataques preemptivos, e foi mais longe advogando pela legitimidade de ataques preventivos[67]. Um ataque preemptivo é realizado quando um ataque é iminente; um ataque preventivo é realizado para evitar

---

[64] Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*.

[65] Devanny, "The Ethics of Offensive Cyber Operations."

[66] Pereira, "A Legítima Defesa No Direito Internacional Contemporâneo."

[67] Bush, "The National Security Strategy United States of America."

que o inimigo possa atacar em um futuro não iminente. Não obstante tal diferenciação, ambos são realizados antes que ocorra um ataque inimigo e, portanto, não podem ser considerados legítima defesa de acordo com o quadro legalmente aceito[68].

Os exemplos acima mostram que valores culturais, morais, éticos e outros institucionalizados (e tabus, possivelmente) permeiam a discussão sobre o uso de cibercapacidades ofensivas.

Apesar disso, a maioria dos escritos sobre C-DbN pressupõe negociações em fóruns internacionais e a existência de instrumentos jurídicos (tratados, acordos ou leis internacionais). Esses instrumentos são frequentemente citados nas estratégias nacionais de ciberdefesa e cibersegurança. Não surpreendentemente, muito mais frequentemente nas de nações não-agressivas do que nas das agressivas.

Muito esforço tem sido feito em fóruns internacionais na discussão de normas para regular as ciberoperações. Em novembro de 2019, a Assembleia da ONU aprovou duas propostas distintas para debater a regulamentação das atividades do ciberespaço: uma dos EUA, criando mais um Grupo de Especialistas Governamentais (*Group of Government Experts*, GGE); e outra da Rússia, criando um Grupo de Trabalho Aberto (*Open-Ended Working Group*, OEWG)[69].

GGEs são comuns na rotina da ONU, constituídos *ad hoc* quando algum assunto merece atenção da ONU, com especialistas de 15 a 25 países, mas raramente são bem-

[68] Pereira, "A Legítima Defesa No Direito Internacional Contemporâneo."

[69] Achten, "New U.N. Debate on Cybersecurity in the Context of International Security"; Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased"; Colatin, "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace."

sucedidos[70]. GGEs relacionados à regulação cibernética também não são novidade. Os de 2004-5 e 2009-10 não obtiveram resultados significativos. No entanto, o de 2012-13 teve sucesso considerável. Pela primeira vez, 15 países, incluindo Rússia, China, EUA, Índia, Reino Unido, França e Alemanha, chegaram ao entendimento de que o *jus ad bellum* (Carta da ONU) se aplicaria ao ciberespaço, embora não tenha havido acordo sobre *jus in bello* (Direito Internacional Humanitário – DIH – ou Direito Internacional dos Conflitos Armados – DICA). O GGE 2014-15 desenvolveu novas regras para orientar a atividade dos Estados no ciberespaço em tempos de paz, mas não obteve o mesmo sucesso de seu antecessor, como pretendiam os EUA[71].

OEWGs, por sua vez, são fóruns abertos a todas as nações. Os EUA se opuseram à criação deste argumentando que a existência de dois grupos de discussão separados dividiria esforços e que a intenção da Rússia era, em um fórum mais amplo, atrasar a discussão[72]. No entanto, já em 1998, a Rússia fora a primeira nação a propor um tratado internacional da ONU para proibir armas eletrônicas e informacionais (inclusive para fins de propaganda), que poderiam ser usadas para "afetar negativamente a segurança dos Estados", com uma resolução aprovada pela Assembleia Geral[73]. Em 2011,

---

[70] Nye, "How Will New Cybersecurity Norms Develop?"; Achten, "New U.N. Debate on Cybersecurity in the Context of International Security."

[71] Grigsby, "The End of Cyber Norms"; Fidler, "The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions Than Answers."

[72] Achten, "New U.N. Debate on Cybersecurity in the Context of International Security"; Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased"; Colatin, "A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace."

[73] Grigsby, "The End of Cyber Norms"; Nye, "How Will New Cybersecurity Norms Develop?"

Rússia, China, Tadjiquistão e Uzbequistão propuseram que a ONU regulasse "a divulgação de informações incompatíveis com a política interna e a estabilidade social e econômica dos países, bem como seu ambiente cultural e social"[74].

Sob qualquer perspectiva, porém, a aprovação da criação desses dois grupos pela Assembleia Geral da ONU mostra que a preocupação internacional com o tema é geral e que os argumentos de ambos os lados estão sendo ouvidos. Essa preocupação também é evidente em outras iniciativas.

Uma questão chave no debate é a aplicabilidade do atual *jus ad bellum* e *jus in bello* às ciberatividades. Por um lado, argumenta-se que, na ausência de regras específicas, os Estados devem trabalhar por analogia, seja equiparando ciberataques a ataques armados tradicionais e tratando-os sob as leis dos conflitos armados ou equiparando-os a atividades criminosas e lidando com eles na forma das leis criminais internas[75]. Os EUA e seus aliados, principalmente na OTAN, são favoráveis a esse argumento, embora alguns princípios fundamentais permaneçam sem solução, como o que seria um ciberataque ou caracterizaria o uso da força no ciberespaço. Por outro lado, Rússia, China e Brasil, entre outros, manifestam considerável relutância em concordar com a aplicabilidade de regras não específicas, considerando a necessidade de acordos específicos como um imperativo[76].

Foi no contexto da aplicabilidade da norma vigente que, sob os auspícios da NATO, um grupo internacional de acadêmicos produziu o *Tallinn Manual on the International Law Applicable to Cyber Warfare* [77]. O trabalho foi posteriormente ampliado com o Projeto "Tallinn 2.0",

---

[74] Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace."

[75] Sklerov, "Responding to International Cyber Attacks."

[76] Giles and Monaghan, "Legality in Cyberspace: An Adversary View"; Schmitt and Vihul, "The Nature of International Law Cyber Norms."

[77] Schmitt, *Tallinn Man. Int. Law Appl. to Cyber Warf.*

publicado quatro anos depois, repleto de exemplos que ilustram uma interpretação da aplicação das regras atuais às ciberoperações [78] . Os chineses, de forma frequente, argumentam que a iniciativa é um exemplo claro de uma tentativa de legalizar o uso militar do ciberespaço pelas potências ocidentais[79].

Embora a doutrina seja uma fonte secundária do direito internacional, ela constitui um elemento "altamente persuasivo" na interpretação da disposição dos tratados e na identificação do costume internacional. Uma doutrina comum a vários Estados pode evoluir para um "princípio jurídico geral reconhecido pelas nações civilizadas" (*jus cogens*), e depois evoluir para um costume [80] . Portanto, na ausência de convenções ou costumes relacionados aos ciberconflitos, trabalhos acadêmicos como o Manual de Tallinn podem ser uma ferramenta relevante para identificar e formatar normas jurídicas para o ciberespaço[81]. E isso pode ser contrário aos interesses daqueles que se opõem à primazia dos EUA.

Desde 2010, os EUA têm sido relativamente bem-sucedidos em conseguir que algumas das principais ciberpotências concordem com um conjunto cada vez mais prescritivo de regras sobre o que podem e não podem aplicar no ciberespaço. No entanto, o processo falhou em obter consentimento explícito para a aplicabilidade das leis de guerra aos ciberconflitos. Entre outros, Rússia, China e Cuba

---

[78] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable To Cyber Operations*.

[79] Huang and Mačák, "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches"; Henriksen, "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace."

[80] ICJ, "Statute of the International Court of Justice."

[81] Schmitt and Vihul, "The Nature of International Law Cyber Norms."

se recusaram a fazê-lo, sob a suspeita de que isso constituiria uma "luz verde" para ações hostis no ciberespaço[82].

No entanto, não apenas os opositores tradicionais dos EUA discordam em alguns aspectos da aplicabilidade das leis internacionais existentes. Até mesmo os membros da OTAN trabalham para moldar a formação do direito consuetudinário, expressando suas opiniões particulares (e frequentemente conflitantes) em aspectos fundamentais[83].

No final, "normas [e instituições] podem impor custos a um atacante mesmo que o ataque não seja negado pela defesa e não haja retaliação"[84].

6.6 Emaranhamento (*Entanglement*)

DbE é outro conceito que surgiu do interesse renovado em pesquisas de dissuasão advindas de ciberameaças. Ciber DbE (C-DbE) é a versão cibernética dele. Sua ideia central é que um ciberataque pode "sair pela culatra", impondo custos severos ao próprio agressor devido às suas interdependências com a vítima[85].

> Como a China se beneficia dos mercados dos EUA e da Europa, é dissuadida de prejudicá-los com ciberataques que degradam/negam, destroem ou interrompem, ou de qualquer

[82] Grigsby, "The End of Cyber Norms."

[83] Iran-Armed Forces Cyberspace Center, "General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat"; UK-MoD, "Cyber Prim."; New Zealand, "The Application of International Law to State Activity in Cyberspace"; France-Ministère des Armées, "International Law Applied to Operations in Cyberspace"; Nederlands-MoFA, "Appendix: International Law in Cyberspace"; Australia-Department of Foreign Affairs and Trade, "Australia's International Cyber Engagement Strategy."

[84] Nye, "Deterrence and Dissuasion in Cyberspace."

[85] Nye, "Can China Be Deterred in Cyber Space?"

> forma prejudicam seus benefícios existentes, tanto no curto quanto no longo prazo.[86]

O conceito se beneficia um pouco do medo da "propagação imprevisível e incontrolável" de malware[87], uma das características das ciberarmas discutidas no Capítulo 4. Como exemplo, o Stuxnet, apesar de ter como alvo as centrífugas iranianas, infectou a instalação em mais de 150 países. Um exemplo mais contemporâneo é o NotPetya. Atribuído publicamente à Rússia por todas as nações que integram o "clube de inteligência" Five Eyes (EUA, Reino Unido, Canadá, Austrália e Nova Zelândia), este malware visava atacar a Ucrânia. No entanto, infectou e danificou computadores em todo o mundo, causando perdas de mais de USD 300 milhões para a gigante de logística FedEx e mais de USD 350 milhões para a Maersk, a maior empresa de transporte do mundo, para citar alguns. As perdas globais estimadas chegam a USD 10 bilhões. Também atingiu a companhia petrolífera estatal russa Rosneft, na própria "mãe Rússia"[88].

6.7 Individualização

A Ciberdissuasão por Individualização (C-DbI) é o terceiro novo tipo de dissuasão nascido no debate da ciberdissuasão. O conceito foi desenvolvido a partir de uma iniciativa da administração do Presidente Obama em 2015.

> A aplicação da lei também pode ser um impedimento eficaz para ciberameaças, tanto por meio da negação (por exemplo, derrubar uma botnet criminosa que pode ser usada em um ataque) quanto pela imposição de custos (por exemplo, prender os perpetradores de

[86] Brantly, "Entanglement in Cyberspace: Minding the Deterrence Gap."

[87] Malagutti, "State-Sponsored Cyber-Offences."

[88] Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."

> ciberataques). Embora a investigação e o processo sejam desafiadores no contexto cibernético, o governo dos Estados Unidos usa essa ferramenta de forma eficaz para interromper e degradar as cibercapacidades do adversário.[89]

Ciaran Martin, ex-chefe do National Cyber Security Center (NCSC) britânico, ramo do GCHQ, observou que, em vez da abordagem tradicional de processar criminosos internos, o governo dos EUA adotou uma abordagem diversa.

> A engenhosa inovação do governo Obama de emitir acusações criminais contra atores estatais hostis fez mais para deter a atividade estatal hostil do que qualquer ciberataque de retaliação: não apenas constrangendo os estados que acusavam, mas removendo, para sempre, a perspectiva de viajar para o Ocidente por qualquer motivo, de qualquer dos indiciados.[90]

A C-DbI "foca no que hackers ou invasores individuais provavelmente valorizam e baseia a dissuasão nessa análise individual de custo-benefício" [91]. Como os indivíduos valorizam as coisas de maneira diferente dos Estados, isso deve exercer um impacto mais significativo nos primeiros do que nos últimos [92]. Se um hacker, ou sua família, tem "ambições de viajar ou estudar no exterior, ou de possuir ativos financeiros internacionais, a possibilidade de perder tais oportunidades como resultado de uma escolha de emprego pode forçar uma reflexão"[93].

---

[89] US-White House, "Report on Cyber Deterrence."

[90] Martin, "Cyber-Weapons Are Called Viruses for a Reason : Statecraft and Security in the Digital Age."

[91] Braw and Brown, "Personalised Deterrence of Cyber Aggression."

[92] Braw and Brown.

[93] Braw and Brown.

Acusações desse tipo foram emitidas em 2018, quando "o Departamento de Justiça dos EUA (DoJ) acusou o norte-coreano Park Jin Hyok de conspirar para realizar ciberataques e intrusões, acusando-o de envolvimento no incidente da Sony", quando o "Departamento dos EUA do Tesouro impôs sanções a ele e contra a *joint-venture* Chosun Expo, ligada ao regime, onde trabalhou"[94].

No mesmo ano de 2018, 12 membros do GRU, a agência de inteligência militar russa, foram indiciados por supostamente estarem envolvidos na interferência nas eleições presidenciais dos EUA de 2016[95].

Em 2019, no entanto, a CrowdStrike, uma empresa de cibersegurança, indicou em sua Análise Anual de Ameaças:

> Em muitos aspectos, 2018 parecia ser um ano marcadamente diferente do anterior. Na ausência de alguns dos eventos de alto perfil observados em 2017, como WannaCry e NotPetya, as manchetes em 2018 foram definidas por uma série de acusações do Departamento de Justiça dos EUA (DoJ) contra indivíduos vinculados a adversários nomeados e patrocinados pelo Estado. Possivelmente afetado por essas divulgações públicas, a atividade contínua de desenvolvimento de ferramentas e as mudanças nas táticas, técnicas e procedimentos (TTPs) parecem indicar que 2018 foi um ano de transição para muitos adversários. *Uma coisa estava clara: os esforços de aplicação da lei ainda não interromperam ou dissuadiram as atividades patrocinadas por estados-nação*.[96]

---

[94] Braw and Brown.

[95] Columbia, "Annex B App5 Indictment."

[96] CrowdStrike, "2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed", grifo nosso.

Em outubro de 2020, o Departamento de Justiça dos EUA indiciou seis cidadãos russos, membros da mesma GRU, por sua responsabilidade em vários ciberataques, incluindo: o das eleições presidenciais francesas de 2017; o dos Jogos Olímpicos de Inverno de 2018; o das empresas e instalações de saúde da Pensilvânia (EUA) em 2018; os da rede elétrica ucraniana, em 2015 e 2016; e o NotPetya, em 2017[97].

Um aspecto essencial dessa abordagem individualizada "é sinalizar a probabilidade de consequências específicas para hackers individuais", "divulgar antecipadamente a gama de possíveis consequências e levar a resposta muito além das notificações, indo além de nomear e constranger [*name-and-shame*], nomear, constranger e condenar"[98].

A C-DbI também apresenta menos potencial para "consequências explosivas em caso de erro", uma vez que "permite que os estados evitem o problema de atribuição pegajoso que os estados patrocinadores usaram em seu benefício nas últimas duas décadas"[99].

6.8 Comparando os Diferentes Tipos de Dissuasão

Snyder[100] propôs uma comparação entre os dois tipos de "dissuasão" então definidos: "por Punição" e "por Negação". Seu modelo considerou quatro parâmetros e seus pesos relativos, classificados em três graus (Baixo, Constante ou Alto) para cada tipo de dissuasão, visto da perspectiva do atacante. O resultado pode ser encontrado na Tabela 6-1.

Os objetivos de Snyder pareciam destinados a ser mais esclarecedores do que metodologicamente rigorosos. Apesar

---

[97] Schmidt and Perlroth, "U.S. Charges Russian Intelligence Officers in Major Cyberattacks."

[98] Braw and Brown, "Personalised Deterrence of Cyber Aggression."

[99] Braw and Brown.

[100] Snyder, "Deterrence by Denial and Punishment."

disso, sua tentativa sugere um modelo para comparar os seis tipos de uma "Teoria da Dissuasão" mais ampla.

Tabela 6-1 – Comparação entre Punição e Negação

Parâmetro	Punição	Negação
Credibilidade da ameaça	Geralmente Baixo	Alto
Custos resultantes da resposta	Alto	Relativamente Baixo
Valorização do "prêmio"	Constante	Constante
Probabilidade de sucesso do ataque	Alto	Baixo

Fonte: Compilada pelo autor baseada em Snyder[101]

A Tabela 6-2 apresenta uma comparação, considerando os achados desta pesquisa relacionados aos elementos conceituais descritos neste capítulo, sob a perspectiva do dissuasor.

Células vazias significam "Não Aplicável" ou "Irrelevante". No que se refere à "Soberania", "Alta" e "Baixa" indicam o possível impacto resultante de alegações de violação de soberania por parte dos dissuadidos. A linha denominada "Ferramental (Armas)" apresenta a classe de software necessário para implementar esse tipo de dissuasão (Ofensivo, Defensivo ou Forense). No tocante à "Causação", indica-se o tipo de causação possível (Positiva ou Negativa). Quanto à "Cultura", reflete o tipo de cultura ou tradição necessária ("Agressiva" ou "Não-Agressiva). Já no caso da linha "Assimetria", os valores indicam a tendência do dissuadido desafiar o dissuasor. Em outras palavras, espera-se que o dissuasor seja mais desafiado por forças menores ao implementar a C-DbP (como no exemplo do Irã e da Coreia do

[101] Snyder.

Norte desafiando os EUA). Nos demais elementos, os valores são autoexplicativos.

Tabela 6-2 – Comparação Entre os Seis Tipos de Ciberdissuasão

Elemento	**C-DbP**	**C-DbD**	**C-DbF**	**C-DbN**	**C-DbE**	**C-DbI**
Soberania	Baixo	Alto		Alto		
Ferramental (Armas)	Ofensivos	Defensivos		Forenses		Forenses
Causação	Positiva/ Negativa	Negativa	Negativa	Negativa	Negativa	Negativa
Cultura	Agressiva	Não-Agressiva				
Atribuição	Alto			Médio		Alto
Assimetria	Alto	Médio				Médio
Resiliência	Baixo	Alto				
Sinalização	Alto	Baixo				Alto
Persuasão	Alto	Baixo				
Dissuasão	Baixo	Alto	Baixo	Médio	Alto	Alto
Capacidades	Alto	Alto	Alto	Baixo	Baixo	Alto
Vontade	Alto	Médio	Baixo	Baixo	Baixo	Médio
Credibilidade	Alto	Médio	Médio	Baixo	Baixo	Médio

Fonte: Compilada pelo autor

Elemento	C-DbP	C-DbD	C-DbF	C-DbN	C-DbE	C-DbI
Soberania						
Ferramental (Armas)						
Causação						
Cultura						
Atribuição						
Assimetria						
Resiliência						
Sinalização						
Persuasão						
Dissuasão						
Capacidades						
Vontade						
Credibilidade						

Fonte: Compilada pelo autor

6.9 Conclusão

A ciberdissuasão ainda é um campo incipiente de pesquisa (e prática). No entanto, evidências empíricas mostram que a tradicional opção de dissuasão por (ameaça de) punição (C-DbP) não gerou os efeitos esperados das lições de história da Guerra Fria. A opção pela C-DbD, apesar das dificuldades, nomeadamente aquelas relacionadas com o custo de desenvolvimento e implantação e gestão de defesas adequadas, ainda parece ser a melhor opção, sobretudo quando o dissuasor não dispõe de um quadro institucional que suporte ações ofensivas. A C-DbF não parece ser promissora, exceto quando a assimetria é tão significativa que descaracteriza a competição.

A C-DbN tende a se consolidar somente a médio e longo prazos. Ainda assim, é uma opção promissora, embora as dificuldades observadas nas negociações dos GGEs e do OEWG indiquem um caminho ainda bastante tortuoso. Já a C-DbE continua a ser um campo teórico de pesquisa. O caso NotPetya, que saiu pela culatra na Rússia, pode ter servido de lição, embora ainda não seja possível garantir isso. Por fim, a C-DbI tem sua eficácia questionada posto que indiciados de nações como Rússia, Coréia do Norte e China têm perspectivas relativamente baixas de realmente virem a sofrer as sanções estipuladas por tribunais estrangeiros. No entanto, à medida que o mecanismo se estabelece e atinge as empresas e organizações para as quais os indivíduos trabalham, o prejuízo ao *soft power* de seus respectivos países pode causar algum reflexo relevante.

A questão mais importante, no entanto, é que esses tipos de ciberdissuasão não são mutuamente exclusivos. Eles podem, e devem, ser exercidos em conjunto, considerando meios, objetivos e a cultura do dissuasor e do dissadido.

7 Conclusões

Este livro apresentou, de forma didática, elementos cruciais para a compreensão da relevância do Software Power para a defesa e segurança nacionais contemporâneas.

Primeiro, demonstrou que existem várias razões pelas quais um aspirante a ciberpotência deva se concentrar no Poder de Software em vez de no Poder de Hardware, ainda que seja bastante improvável que um país que planeje desenvolver cibercapacidades avançadas possa fazê-lo em todas as camadas de software existentes, pelo menos no curto prazo. Mostrou, também, que alcançar conhecimento avançado ao menos nos níveis superiores do software usado garante uma escala muito menor de risco cibernético e uma "superfície de ataque" muito menor, em um ritmo muito mais rápido e com menor custo do que tentar competir no nível do hardware.

Segundo, mostrou que uma análise criteriosa da literatura disponível sobre ciberpoder mostra que ela reflete uma postura agressiva, baseada na necessidade de ferramentas de ataque que podem tanto incutir medo quanto impor sua dominância no ciberespaço, utilizada com frequência como elemento de estadismo. Deixou caro, também, que na economia globalizada dos dias de hoje, uma nação com a proeminência econômica internacional do Brasil mantém relações em diversos compôs com todas as nações podem ter interesses conflitantes com vários países comumente citados como cibersuperpotências. Assim, há a necessidade de proteger os interesses do país tendo em mente o ciberpoder, e a intenção de usá-lo, por esses atores, requerendo preparação, planejamento e investimentos de longo prazo, típicos em questões de segurança e defesa nacional.

Terceiro, apresentou-se as características peculiares das ciberarmas, que fazem com que devam ser consideradas de forma inerentemente diversa daquelas das armas cinéticas (e

mesmo estratégicas) até hoje conhecidas e profundamente estudadas. Onde foram debatidos aspectos da natureza única das ciberarmas, incluindo sua anatomia e sua natureza, bem como dos riscos de seu uso, e o desenvolvimento de ciberarmas cada vez mais inteligentes e autônomas. Foram tratados também temas como indicadores de comprometimento, assimetria de poder, e a natureza efêmera, imprevisível e incontrolável das ciberarmas, mostrando que a necessidade de exploração cada vez mais rápida das vulnerabilidades cibernéticas torna tais características cada vez mais perigosas.

Quarto, buscou-se conceituar a que seria a ciberdissuasão e sua importância para a proteção da segurança nacional no ciberespaço, e mesmo fora dele, discutindo-se a necessidade da ciberdissuasão como um tópico crescente de pesquisa, associada ao crescimento da importância dos computadores nas economias e sociedades modernas, e apresentando-se a correlação entre a segurança nacional e o ciberespaço, bem como a aplicabilidade dos conceitos de dissuasão clássica (entendida como mais que a "simples" deterrência) ao ciberespaço, e analisada a possibilidade de uso do quinto domínio da guerra como um instrumento de coerção ou coação, e a ausência da ciberdissuasão na doutrina brasileira

Quinto, mostrou-se que a ciberdissuasão ainda é um campo incipiente de pesquisa (e prática) no mundo todo, mas que evidências empíricas mostram que a tradicional opção de dissuasão por (ameaça de) punição (C-DbP) não gerou os efeitos esperados das lições de história da Guerra Fria. Enquanto a opção pela C-DbD, apesar das dificuldades, nomeadamente as relacionadas com o custo de desenvolvimento e implantação e gestão de defesas adequadas, ainda parece ser a melhor opção, sobretudo quando o dissuasor não dispõe de um quadro institucional que suporte as ações ofensivas.

Outrossim, este livro se propôs a oferecer uma base para iniciar um debate ainda incipiente, mas cada vez mais relevante para as pretensões de inserção internacional do Brasil num momento em que se intensifica a importância dos computadores e redes na consolidação da chamada Era do Conhecimento.

Página intencionalmente deixada em branco.

8 Referências

8.1 Capítulo 01 – Prelúdio

Austin, Greg. “Sino-US tensions in Cyberspace: All China’s fault?” *The Diplomat*, 2015. http://thediplomat.com/2015/09/sino-us-tensions-in-cyberspace-all-chinas-fault/.

Brasil-MD. “Política Nacional de Defesa e Estratégia Nacional de Defesa”. Brasília, 2020.

Clausewitz, Carl von. *On War*. Organizado por Michael Howard e Peter Paret. Princeton: Princeton University Press, 1976.

Comissão Europeia. “Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE - Comunicação Conjunta ao Parlamento Europeu e ao Conselho”. Bruxelas, 2017.

Falliere, Nicolas, Liam O Murchu, e Eric Chien. “W32.Stuxnet Dossier”. *Symantec-Security Response*. Vol. Version 1., 2011. https://doi.org/20 September 2015.

Gompert, David, e Hans Binnendijk. “Time for Washington to amp up the power to coerce”. *War On The Rocks*, 2016.

Greenwald, Glenn. No place to hide: Edward Snowden, the NSA and the surveillance state. Penguin Books, 2014.

Harris, Shane. @War: The rise of the Military-Internet complex. Boston, 2014.

Houaiss, Antônio, e Mauro Villar. *Dicionário Houaiss da Língua Portuguesa*. Rio de Janeiro: Editora Objetiva, 2001.

Krever, Mick, e Laura Smith-Spark. “Lavrov denies Russian influence over US election”. *CNN*, 2016.

Mazarr, Michael. “The world has passed the old grand strategies by”. *War On The Rocks*, 2016.

Nye, Joseph. “International Norms in Cyberspace”. *Project Syndicate*, 2015.

Paletta, Damian. “U.S. Blames Russia for recent hacks”. *The Wall Street Journal*, 2016.

Parlamento Europeu. “RELATÓRIO sobre ciberdefesa (2018/2004(INI)) - A8-0189/2018”, 2018.

Rid, Thomas. *Cyber War Will Not Take Place*. *Journal of Strategic Studies*. Vol. 35. New york: Oxford University Press, USA, 2013. https://doi.org/10.1080/01402390.2011.608939.

Schelling, Thomas. *Arms and influence: With a new preface and Afterword*. Yale University Press, 2008.

———. *The Strategy of Conflict*. Harvard University Press, 1980.

Wagstyl, Stefan. “Germany points finger at Kremlin for cyber attack on the Bundestag”. *Financial Times*. 2016.

8.2 Capítulo 02 – Software Power

Angelo, Cláudio. “‘Eixo do mal’ científico: Ministério pede explicações à Dell sobre exigências a físicos”. *Folha de São Paulo*. 14 de setembro de 2007. http://www1.folha.uol.com.br/fsp/ciencia/fe1409200703.htm.

Apache Software Foundation. “Apache Accumulo”. Apache Accumulo website, 2020. https://accumulo.apache.org/.

———. “Apache Hadoop”. Apache Hadoop website, 2020. http://hadoop.apache.org/.

Betz, David, e Tim Stevens. *Cyberspace and the state: Towards a strategy for Cyberpower*. Routledge for the International Institute for Strategic Studies (IISS), 2011.

Biercuk, Michael J, e Richard Fontaine. “The Leap into Quantum Technology: A Primer for National Security Professionals”. *War On The Rocks*, 2017, 1–13.

BOINC. “BOINC”. BOINC website, [s.d.]. https://boinc.berkeley.edu/.

Churchill, Winston. *The Second World War, Volume 1: The Gathering Storm*. Mariner Books, 1986.

Clark, Don. “U.S. Agencies block technology exports for supercomputer in China”. *The Wall Street Journal*, 2015.

Dean, Jeffrey, e Sanjay Ghemawat. “MapReduce: Simplified Data Processing on Large Clusters”. *OSDI04: Sixth Symposium on Operating System Design and Implementation* 51, nº 1 (2004): 107. https://doi.org/10.1145/1327452.1327492.

European Comission. “High-Performance Computing”. European Comission, 2017.

———. “High Performance Computing (HPC) Factsheet”. European Comission, 2017.

Fell, Andy, e Bevan Bass. “World ’ s First 1,000-Processor Chip”. *UC Davis News*. 2016.

Financial Times. “Quantum computing rivals muster software power in new ‘ arms race ’”. *Financial Times*, 2017.

Folding@home. “Folding@home stats report”, [s.d.]. https://stats.foldingathome.org/os.

———. “Front Page - Folding@home”, [s.d.]. https://foldingathome.org/home/.

Freedman, Lawrence. *Strategy: A history*. Oxford: Oxford University Press, 2015.

Fu, Haohuan, Junfeng Liao, Jinzhe Yang, Lanning Wang, Zhenya Song, Xiaomeng Huang, Chao Yang, et al. “The Sunway TaihuLight supercomputer: system and applications”. *Science China Information Sciences* 59, nº 7 (2016): 1–16. https://doi.org/10.1007/s11432-016-5588-7.

Gama Neto, Ricardo. “Guerra cibernética/Guerra eletrônica – conceitos, desafios e espaços de interação”. *Revista Política Hoje* 26, nº 1 (2017): 201–18.

Gama Neto, Ricardo, e Gils Lopes. “Armas Cibernéticas e Segurança Nacional”. In *Segurança e Defesa Cibernética: da fronteira física aos muros virtuais*, organizado por Oscar Mederios Filho, Walfredo B Ferreira Gonzalez Neto, e Selma Lúcia de Moura. Editora UFPE, 2014.

Guedes de Oliveira, Marcos Aurelio, e Lucas Soares Portela. “As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil”. *Revista Brasileira de Estudos de Defesa* 4, nº 2 (2017): 77–99. https://doi.org/10.26792/rbed.v4n2.2017.75014.

Harris, Shane. *@War: The rise of the Military-Internet complex*. Boston, 2014.

Klimburg, Alexander, e Heli Tirmaa-Klaar. “Cybersecurity and Cyberpower : Concepts , Conditions and Capabilities for Action Wihtin the EU”. Brussels, 2011.

Kuehl, Daniel. “From Cyberspace to Cyberpower: Defining the Problem”. In *Cyberpower and National Security*. National Defense University Press, 2009.

Libicki, Martin. “Cyberdeterrence and Cyberwar”. RAND Corporation, 2009.

Lukasik, Stephen J. “A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains”. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*, organizado por National Research Council (U.S.). Committee on Deterring Cyberattacks: Informing Strategies e Developing Options for U.S. Policy, 99–121. National Academies Press, 2010.

Malagutti, Marcelo. *Ciberdefesa e Cibersegurança: Um Olhar Brasileiro*. Brasília: Instituto Vegetius, 2022.

———. “Software Power”. Strife, 2016. http://www.strifeblog.org/2016/11/02/cybersecurity-in-practice-part-i-software-power/.

Metz, Cade. “NSA mimics Google, Pisses off senate”. *Wired*, 2012. http://www.wired.com/2012/07/nsa-accumulo-google-bigtable/.

Moon, Angela. “Exclusive: Google suspends some business with Huawei after Trump blacklist - source - Reuters”. *Reuters*, 2019.

Nye, Joseph. *Soft Power: The Means To Success In World Politics*. New York, NY: Public Affairs, 2004.

Owen, Taylor, e Robert Gorwa. “Quantum Leap: China’s Satellite and the New Arms Race”. *Foreign Affairs*, 2016.

Shidong, Zhang. “China offers five-year tax breaks to chip makers, software developers to bolster industry as trade war stretches to tech”. *South China Morning Post*. 2019.

Stevens, Tim, e David Betz. “Analogical Reasoning and Cyber Security”. *Security Dialogue* 44, nº 2 (2013): 147–64.

Strumpf, Dan. “Huawei’s 5G Dominance Threatened by U.S. Policy on Chips - WSJ”. *The Wall Street Journal*. 2020.

The Economist. “After Moore’s Law”. *The Economist*. London, 2016.

———. “The world’s most valuable resource is no longer oil, but data”. *The Economist*, maio de 2017.

TOP500.org. “Top500 June 2016”. TOP500.org, 2016. https://www.top500.org/lists/2016/06/.

———. “Top500 June 2018”. TOP500.org, 2018. https://www.top500.org/lists/2018/06/.

———. “Top500 November 2015”. TOP500.org, 2015. https://www.top500.org/lists/2015/11/.

———. “TOP500 November 2020”. TOP500.org, 2020. https://top500.org/top500/lists/2020/11/.

———. “TOP500 November 2021”. TOP500.org, 2021. https://top500.org/lists/top500/2021/11/.

UK-GCHQ. *HIMR Data Mining Research Problem Book*. GCHQ, 2011.

US-DoC. “Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List | U.S. Department of Commerce”. Dept. of Commerce Press Releases, 2020. https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd.

US-White House. “The Trump Administration Is Investing $1 Billion in Research Institutes to Advance Industries of the Future | The White House”. White House website, 2020. https://www.whitehouse.gov/articles/trump-administration-investing-1-billion-research-institutes-advance-industries-future/.

Yang, Yuan, e Nian Liu. “Beijing orders state offices to replace foreign PCs and software”. *Financial Times*, 2019.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York: Crown, 2015.

8.3 Capítulo 03 – Ciberofensas Patrocinadas por Estados

Adams, James. “Virtual Defense”. *Foreign Affairs* 80, nº 3 (2001): 98. https://doi.org/10.2307/20050154.

Arquilla, John. “From Blitzkrieg to Bitskrieg: The Military Encounter with Computers”. *Communications of the ACM* 54, nº 10 (2011): 58. https://doi.org/10.1145/2001269.2001287.

Arquilla, John, e David Ronfeldt. “Cyberwar is coming!” *Comparative Strategy* 12, nº 2 (1993): 141–65. https://doi.org/10.1080/01495939308402915.

Austin, Greg. “Strategic culture and Cyberspace: Cyber militias in peacetime?” *The Diplomat*, 2016. http://thediplomat.com/2016/02/strategic-culture-and-cyberspace-cyber-militias-in-peacetime/.

Betz, David, e Tim Stevens. *Cyberspace and the state: Towards a strategy for Cyberpower*. Routledge for the International Institute for Strategic Studies (IISS), 2011.

Campbell, Duncan. *Development of Surveillance Technology and Risk of Abuse of Economic Information Part 2/5*, 1999. http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf.

Cilluffo, Frank, Sharon Cardash, e George Salmoiraghi. “A Blueprint for Cyber Deterrence: Building Stability through Strenght”. *Military and Strategic Affairs* 4, nº 3 (2012): 3–23.

CISCO. “What Is an Advanced Persistent Threat (APT)?” CISCO Website. Acessado 4 de fevereiro de 2021. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html.

Clarke, Richard A, e Robert K Knake. *Cyber war: The next threat to national security and what to do about it*. New York: HarperCollins Publishers, 2010.

Clausewitz, Carl von. *On War*. Organizado por Michael Howard e Peter Paret. Princeton: Princeton University Press, 1976.

Damião, Rui. “Ciberhigiene: a base da saúde de uma organização”. *IT Insight*, 12 de março de 2021. https://www.itinsight.pt/news/seguranca/ciberhigiene-a-base-da-saude-de-uma-organizacao.

Davis, Paul. “Deterrence, Influence, Cyber Attack and Cyberwar”. *International Law and Politics* 47, nº 327 (2015): 327–55.

Denning, Dorothy. “Rethinking the Cyber Domain and Deterrence”. *Joint Forces Quarterly* 77, nº 2nd Quarter (2015): 8–15.

Deutsche Welle. “German intelligence services ′alarmed′ about potential Russian interference in elections”. *Deutsche Welle*, 16 de novembro de 2016.

Falliere, Nicolas, Liam O Murchu, e Eric Chien. “W32.Stuxnet Dossier”. *Symantec-Security Response*. Vol. Version 1., 2011. https://doi.org/20 September 2015.

FireEye/Mandiant. “M-Trends 2021 Report”. *M-Trends*, 2021. https://www.fireeye.com/current-threats/annual-threat-report.html.

Follath, Erich, e Holger Stark. “The Story of ‘Operation Orchard’: How Israel Destroyed Syria’s Al Kibar Nuclear Reactor - DER SPIEGEL”. *Der Spiegel*, 2 de novembro de 2009. https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

Freedman, Lawrence. *Strategy: A history*. Oxford: Oxford University Press, 2015.

GovCERT.ch. “APT case RUAG technical report”, 2016. https://www.melani.admin.ch/dam/melani/it/dokumente/2016/technical report ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf.

Greenwald, Glenn. *No place to hide: Edward Snowden, the NSA and the surveillance state*. Penguin Books, 2014.

Hare, Forrest. “The significance of attribution to cyberspace coercion: A political perspective”. In *CyCon 2012*, 1–15. Tallinn: CCDCOE, 2012.

Harris, Shane. *@War: The rise of the Military-Internet complex*. Boston, 2014.

HM Government. “Equipment interference code of practice pursuant to section 71 of the regulation of Investigatory powers act 2000”. London, 2016.

———. “Operational Case for Bulk Powers”, 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

Howard, Michael. *Clausewitz: A Very Short Introduction*. Oxford: Oxford University Press, 2002.

Kaspersky. “What Is an Advanced Persistent Threat (APT)?” Kaspersky Website. Acessado 4 de fevereiro de 2021. https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats.

Kedmey, Dan. “Report: NSA authorized to spy on 193 countries”. *Time*, 2014. http://time.com/2945037/nsa-surveillance-193-countries/.

Khandelwal, Swati. “U.S. Supreme court allows the FBI to hack any computer in the world”. *The Hacker News*, 2016. http://thehackernews.com/2016/04/fbi-hacking-power.html.

Kissinger, Henry. *World Order*. New York: Penguin Group (USA), 2014.

Klimburg, Alexander, e Heli Tirmaa-Klaar. “Cybersecurity and Cyberpower : Concepts , Conditions and Capabilities for Action Wihtin the EU”. Brussels, 2011.

Kopp, Carlo. “The Four Strategies of Information Warfare and their Applications”. *IO Journal* 1, nº 4 (2010): 28–33.

Krever, Mick, e Laura Smith-Spark. “Lavrov denies Russian influence over US election”. *CNN*, 2016.

Libicki, Martin. “Cyberdeterrence and Cyberwar”. RAND Corporation, 2009.

———. “Cyberspace is not a Warfighting Domain”. *I/S: A Journal of Law and Policy for the Information Society* 8, nº 2 (2012): 321–36.

Liff, Adam. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War”. *Journal of Strategic Studies* 35, nº 3 (2012): 401–28. https://doi.org/10.1080/01402390.2012.663252.

Lynn, William. “Defending a New Domain: The Pentagon’s Cyberstrategy”. *Foreign Affairs* 89, nº 5 (2010).

Mahnken, Thomas. “Cyberwar and Cyber Warfare”. In *America’s Cyber Future Security and Prosperity in the Information Age (Vol II)*, organizado por Kristin Lord e Travis Sharp, 1º ed. CNAS, 2011.

Mahnken, Thomas, Kristin Lord, e Travis Sharp. *Cyber War and Cyber Warfare*, 2011. http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume II_2.pdf.

Malagutti, Marcelo. “O Papel da Dissuasão no Tocante a Ofensas Cibernéticas”. *Doutrina Militar Terrestre em Revista* 9 (2016): 18–27.

Mandiant. “APT1 Exposing One of China’s Cyber Espionage Units”. *Report*, 2013, 1–76. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Mazzetti, Mark, e David Sanger. “U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict”. *The New York Times*. 2016. http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Mendell, Ronald. “advanced persistent threat | information technology | Britannica”. Encyclopedia Britannica, 25 de julho de 2011. https://www.britannica.com/topic/advanced-persistent-threat.

Morgan, Patrick. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm”. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*, 55–76. National Academies Press, 2010.

Murdock, Jason. “Cyber-espionage: Norway’s intelligence chief accuses china of stealing military secrets”. *Technology*, 2016. http://www.ibtimes.co.uk/cyber-espionage-norways-intelligence-chief-accuses-china-stealing-military-secrets-1546879.

Nichols, Michelle. “North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report | Reuters”. *Reuters*, 6 de agosto de 2019. https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX.

NIST-CSRC. “advanced persistent threat (APT) - Glossary | CSRC”. NIST/CSRC Website. Acessado 4 de fevereiro de 2021. https://csrc.nist.gov/glossary/term/advanced_persistent_threat.

“North Korea: Missile programme funded through stolen crypto, UN report says”. *BBC News*, 6 de fevereiro de 2022. https://www.bbc.com/news/world-asia-60281129.

Omand, David. “Understanding digital intelligence and the norms that might govern it”, 2015. https://www.cigionline.org/sites/default/files/gcig_paper_no8.pdf.

Paletta, Damian. “U.S. Blames Russia for recent hacks”. *The Wall Street Journal*, 2016.

Perlroth, Nicole. “Chinese Hackers Infiltrate New York Times Computers”. *The New York Times*. 30 de janeiro de 2013. https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

Perlroth, Nicole, e Michael Corkery. “North Korea linked to digital attacks on global banks”. *The New York Times*, 2016. http://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html.

Rid, Thomas. *Cyber War Will Not Take Place*. *Journal of Strategic Studies*. Vol. 35. New york: Oxford University Press, USA, 2013. https://doi.org/10.1080/01402390.2011.608939.

Rid, Thomas, e Peter McBurney. “Cyber-Weapons”. *The RUSI Journal* 157, nº 1 (2012): 6–13. https://doi.org/10.1080/03071847.2012.664354.

Rieder, Felix. “Advanced Persistent Threat”. Deloitte Website, 2016. https://www2.deloitte.com/ch/en/pages/risk/articles/advanced-persistent-threat.html.

Russell, Alison. “Strategic anti-access/area denial in cyberspace”. In *7th Cycon*. Tallinn, 2015.

Sanger, David. “Obama ordered wave of Cyberattacks against Iran”. *The New York Times*, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0.

Schneier, Bruce. “Computer Network Exploitation vs. Computer Network Attack”. *Schneier on Security*, 2014. https://www.schneier.com/blog/archives/2014/03/computer_networ.html.

Shalal, Andrea. “U.S. National guard may join cyber offense against Islamic state: Carter”. *Reuters*, 2016. http://www.reuters.com/article/us-usa-military-cyber-idUSKCN0W70UQ.

Sharma, Amit. “Cyber wars: A paradigm Shift from Means to Ends”. *Strategic Analysis* 34, nº 1 (2010): 62–73. https://doi.org/10.1080/09700160903354450.

Singh, Simon. *The Code Book: The Secret History of Codes and Code Breaking*. London: Fourth Estate, 2000.

Stoll, Clifford. *The cuckoo’s egg: Tracking a spy through a maze of computer espionage*. The Bodley Head, London, 1990.

Stone, John. “Cyber war will take place!” *Journal of Strategic Studies* 36, nº 1 (2013): 101–8. https://doi.org/10.1080/01402390.2012.730485.

———. “Technology and war: A Trinitarian analysis”. *Defense & Security Analysis* 23, nº 1 (2007): 27–40. https://doi.org/10.1080/14751790701254441.

Swire, Peter. “US Surveillance Law, Safe Harbor, and Reforms Since 2013”. SSRN, 2015. https://doi.org/10.2139/ssrn.2709619.

TAO Security. “Greg Rattray Invented the Term Advanced Persistent Threat”. TAO Security Blog, 10 de outubro de 2020. https://taosecurity.blogspot.com/2020/10/greg-rattray-invented-term-advanced.html.

TED Talks. *Ralph Kangner: Cracking Stuxnet, a 21st-century cyber weapon*. TED Talks, 2011.

UK-GCHQ/NCSC. “NCSC-certified degrees”. NCSC Website - NCSC.GOV.UK, 20 de dezembro de 2021. https://www.ncsc.gov.uk/information/ncsc-certified-degrees.

UK-GCHQ. “GCHQ History”, 2016.

———. *HIMR Data Mining Research Problem Book*. GCHQ, 2011.

US-JCS. “Information Operations - Joint Publication 3-13”, 2014.

Wagstyl, Stefan. “German security head warns of election interference from Russia”. *Financial Times*. 2016.

———. “Germany points finger at Kremlin for cyber attack on the Bundestag”. *Financial Times*. 2016.

Yadron, Danny. “Supreme court grants FBI massive expansion of powers to hack computers”. *The Guardian*, 2016. https://www.theguardian.com/technology/2016/apr/29/fbi-hacking-computers-warrants-supreme-court-congress.

Zetter, Kim. “Everything We Know About Ukraine’s Power Plant Hack”. *Wired*, 2016.

———. “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History”. *Wired*, 2011.

8.4 Capítulo 04 – Ciberarmas

Adams, James. “Virtual Defense”. *Foreign Affairs* 80, nº 3 (2001): 98. https://doi.org/10.2307/20050154.

Areng, Liina. “Lilliputian States in Digital Affairs and Cyber Security”, 2014.

Arquilla, John. “From Blitzkrieg to Bitskrieg: The Military Encounter with Computers”. *Communications of the ACM* 54, nº 10 (2011): 58. https://doi.org/10.1145/2001269.2001287.

Austin, Greg. “Strategic culture and Cyberspace: Cyber militias in peacetime?” *The Diplomat*, 2016. http://thediplomat.com/2016/02/strategic-culture-and-cyberspace-cyber-militias-in-peacetime/.

Banach, William. “Investigative report on the U.S. National security issues posed by Chinese telecommunications companies Huawei and ZTE”, 2012. https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE Investigative Report (FINAL).pdf.

Brasil-MD-EPEX. “Folder Astros 2020”, [s.d.]. http://www.epex.eb.mil.br/images/pdf/FOLDER-ASTROS.pdf.

Brodie, Bernard. “The Anatomy of Deterrence”. *World Politics* 11, nº 02 (1959): 173–91. https://doi.org/10.2307/2009527.

Calleja, Alejandro, Juan Tapiador, e Juan Caballero. “A look into 30 years of malware development from a software metrics perspective”. In *RAID 2016: Research in Attacks, Intrusion and Defenses*, 9854 LNCS:325–45. Springer Verlag, 2016. https://doi.org/10.1007/978-3-319-45719-2_15.

CTIR Gov. “Indicadores de Comprometimento”. CTIR Gov, 13 de novembro de 2021. https://www.gov.br/ctir/pt-br/assuntos/noticias/2021/indicadores-de-comprometimento.

Dutta, Soumitra, Thierry Geiger, e Bruno Lanvin, orgs. “The Global Information Technology Report 2015”. Geneva, 2015.

Dutta, Soumitra, e Bruno Lanvin, orgs. “Network Readiness Index 2021”. Portulans Institute, 2021.

Falco, Marco. “Stuxnet Facts Report”. Tallinn, 2012.

Galante, Alexandre. “Diferenças entre o submarino Scorpène e o S-BR brasileiro - Poder Naval - Navios de Guerra, Marinhas de Guerra, Aviação Naval, Indústria Naval e Estratégia Marítima”. *Naval*, 7 de dezembro de 2018. https://www.naval.com.br/blog/2018/12/07/diferencas-entre-o-submarino-scorpene-e-o-s-br-brasileiro/.

Gielow, Igor. “FAB compra novos mísseis e quer mais 30 caças Gripen”. *DefesaNet*. 1 de fevereiro de 2022. https://www.defesanet.com.br/f39/noticia/43483/FAB-compra-novos-misseis-e-quer-mais-30-cacas-Gripen/.

Godoy, Roberto. “Míssil de precisão entra em fase final”. *Estadão*, 26 de março de 2023. https://politica.estadao.com.br/noticias/geral,missil-de-precisao-entra-em-fase-final,70002242294.

Harris, Shane. *@War: The rise of the Military-Internet complex*. Boston, 2014.

Hayden, Michael. *Playing to the edge: American intelligence in the age of terror*. New York: The Penguin Press, 2016.

Hutchins, Eric M, Rohan M Amin, e Michael J Cloppert. “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains”, 2010.

IISS. “Artificial Intelligence and Offensive Cyber Weapons”. *Strategic Comments* 25, nº 10 (26 de novembro de 2019): x–xii. https://doi.org/10.1080/13567888.2019.1708069.

Imbel. “Fuzil de Assalto 7,62 IA2”. Imbel Website. Acessado 10 de março de 2022. https://www.imbel.gov.br/index.php/fuzis/93.

Kaspersky Labs. “O que é vírus metamórfico? | Definição de vírus metamórfico”. Kaspersky Labs - Centro de recursos. Acessado 6 de março de 2022. https://www.kaspersky.com.br/resource-center/definitions/metamorphic-virus.

Lee, Robert, e Michael Assante. “The Industrial Control System Cyber Kill Chain”, 2015. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

Libicki, Martin. “Cyberdeterrence and Cyberwar”. RAND Corporation, 2009.

———. “Pulling Punches in Cyberspace”. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*, organizado por National Research Council (U.S.). Committee on Deterring Cyberattacks: Informing Strategies e Developing Options for U.S. Policy, 123–47. National Academies Press, 2010.

Liff, Adam. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War”. *Journal of Strategic Studies* 35, nº 3 (2012): 401–28. https://doi.org/10.1080/01402390.2012.663252.

Lindorfer, Martina, Alessandro Di Federico, Federico Maggi, Paolo Milani Comparetti, e Stefano Zanero. “Lines of malicious code: Insights into the malicious software industry”. *ACM International Conference Proceeding Series*, 2012, 349–58. https://doi.org/10.1145/2420950.2421001.

Lynn, William. “Defending a New Domain: The Pentagon’s Cyberstrategy”. *Foreign Affairs* 89, nº 5 (2010).

Marinha do Brasil. “Submarino Scorpène: A Posição da Marinha”. *DefesaNet*, 22 de dezembro de 2008. https://www.defesanet.com.br/prosub_doc/noticia/31388/MB---SUBMARINO-SCORPENE--A-POSICAO-DA-MARINHA/.

Mearsheimer, John. “The gathering storm: China’s challenge to US power in Asia”. *The Chinese Journal of International Politics* 3, nº 4 (2010): 381–96. https://doi.org/10.1093/cjip/poq016.

Morgan, Patrick. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm”. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*, 55–76. National Academies Press, 2010.

NSA | CSS. “Active Cyber Defense (ACD)”. NSA | CSS Website, 4 de agosto de 2015. https://apps.nsa.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm.

Nye, Joseph. “Cyber War and Peace”. *Project Syndicate*, 2012.

———. “Rules of the Cyber Road for America and Russia”. *Project Syndicate*, 2019.

Rid, Thomas, e Peter McBurney. “Cyber-Weapons”. *The RUSI Journal* 157, nº 1 (2012): 6–13. https://doi.org/10.1080/03071847.2012.664354.

Rumsfeld, Donald H. “Transforming the military”. *Foreign Affairs* 81, nº 3 (2002): 20. https://doi.org/10.2307/20033160.

Saab. “Programa Gripen Brasileiro”. Saab Website. Acessado 10 de março de 2022. https://www.saab.com/pt-br/markets/brasil/gripen-para-o-brasil/programa-gripen-brasileiro.

Sterling, Bruce. “Flame/Stuxnet/Duqu are attacking Kaspersky”. *Wired*, 2015.

Tabansky, Lior. “Basic Concepts in Cyber Warfare”. *Military and Strategic Affairs* 3, nº 1 (2011): 75–92.

TED Talks. *Ralph Kangner: Cracking Stuxnet, a 21st-century cyber weapon*. TED Talks, 2011.

US-DHS. “A Roadmap for Cybersecurity Research”, 2009. https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf.

US-White House. “Presidential Policy Directive/PPD-20”. Washington, 2012.

Valentini, Fernando, e João Dalla Costa. “Leopard 1A5Br - Nova família de blindados sobre lagartas no EB: uma proposta”. DefesaNet, 8 de dezembro de 2017.

https://www.defesanet.com.br/leo/noticia/27904/Nova-familia-de-blindados-sobre-lagartas-no-EB--uma-proposta/.

Zetter, Kim. “Secret Code Found in Juniper’s Firewalls Shows Risk of Government Backdoors”. *Wired*, 2015.

8.5 Capítulo 05 – Ciberdissuasão

Agency, Defense Logistics. “Defense Logistics Agency Strategic Plan 2015-2022.” Vol. 2015, 2015. http://www.strategicmaterials.dla.mil/Pages/default.aspx.

Amin Naves, Guido, and Marcelo Malagutti. “Defesa Cibernética (Ou Ciberdefesa).” In *Dicionário de História, Historiadores e Conceitos Militares*, edited by Francisco Carlos Teixeira da Silva, Bruno de Melo Oliveira, Fernando Velôzo Gomes Pedroza, Francisco Eduardo Alves de Almeida, Paulo André Leira Parente, Ricardo Cabral, and Sandro Teixeira Moita, n.d.

Arquilla, John, and David Ronfeldt. “Cyberwar Is Coming!” *Comparative Strategy* 12, no. 2 (1993): 141–65. https://doi.org/10.1080/01495939308402915.

Auchard, Eric, and Jim Finkle. “Ukraine Utility Cyber Attack Wider than Reported.” *Reuters*, 2016. http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UI23S20160104.

Austin, Greg. “Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security.” In *Asian Security Conference 2016*, 2016.

———. “Strategic Culture and Cyberspace: Cyber Militias in Peacetime?” *The Diplomat*, 2016. http://thediplomat.com/2016/02/strategic-culture-and-cyberspace-cyber-militias-in-peacetime/.

Australia-Department of Foreign Affairs and Trade. “Australia’s International Cyber Engagement Strategy.” *Department of Foreign Affairs and Trade*, 2017. https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT AICES_AccPDF.pdf.

Barlow, John. “A Declaration of the Independence of Cyberspace.” Electronic Frontier Foundation website, 1996. https://www.eff.org/cyberspace-independence.

Barnes, Julian. “U.S. Cyberattack Hurt Iran’s Ability to Target Oil Tankers, Officials Say.” *The New York Times*. 2019. https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

Bell, Daniel. *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. Basic Books, 1976.

Betz, David, and Tim Stevens. *Cyberspace and the State: Towards a Strategy for Cyberpower*. Routledge for the International Institute for Strategic Studies (IISS), 2011.

Brasil-MD. “Política Nacional de Defesa e Estratégia Nacional de Defesa.” Brasília, 2020.

Buchanan, Ben, and Thomas Rid. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1–2 (2014): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Carr, Jeffrey. “Cyber Attacks: Why Retaliating against China Is the Wrong Reaction.” *The Diplomat*, August 2015.

Cilluffo, Frank, Sharon Cardash, and George Salmoiraghi. “A Blueprint for Cyber Deterrence: Building Stability through Strenght.” *Military and Strategic Affairs* 4, no. 3 (2012): 3–23.

Clarke, Richard A, and Robert K Knake. *Cyber War: The next Threat to National Security and What to Do about It*. New York: HarperCollins Publishers, 2010.

Clausewitz, Carl von. *On War*. Edited by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Dragos. “CRASHOVERRIDE: Analyzing the Threat to Electric Grid Operations,” 2017. https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. “W32.Stuxnet Dossier.” *Symantec-Security Response*. Vol. Version 1., 2011. https://doi.org/20 September 2015.

Farrell, Henry, and Charles L Glaser. “The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine.” *Journal of Cybersecurity* 3, no. 1 (2017): 7–17. https://doi.org/10.1093/cybsec/tyw015.

Figueiredo, Nice. “Legislação de Informática No Brasil.” *Revista de Biblioteconomia de Brasília* 34, no. 81 (1986).

Finnemore, Martha, and Duncan B Hollis. “Constructing Norms for Global Cybersecurity.” *American Journal of International Law* 110, no. 3 (2016): 425–79. https://doi.org/10.1017/s0002930000016894.

France-Ministère des Armées. “International Law Applied to Operations in Cyberspace,” 2019. https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

Grimaila, Michael, Robert Mills, and Kevin Beeker. “Applying Deterrence in Cyberspace.” *IO Journal* 1, no. 4 (2010): 21–27.

Guterres, António. “Secretary-General’s Address at the Opening Ceremony of the Munich Security Conference.” Munique: United Nations, 2018. https://www.un.org/sg/en/content/sg/statement/2018-02-16/secretary-general’s-address-opening-ceremony-munich-security.

Hare, Forrest. “The Significance of Attribution to Cyberspace Coercion: A Political Perspective.” In *CyCon 2012*, 1–15. Tallinn: CCDCOE, 2012.

Harris, Shane. *@War*. Boston: Houghton Mifflin, 2014.

Huber, Max. “Reports of International Arbitral Awards Island of Palmas Case (Netherlands, USA).” The Hague, 1928.

Iasiello, Emilio. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security* 7, no. 1 (2014): 54–67. https://doi.org/10.5038/1944-0472.7.1.5.

Jervis, Robert. “Deterrence Theory Revisited.” *World Politics* 31, no. 2 (1979): 289–324.

Khalip, Andrei. “U.N. Chief Urges Global Rules for Cyber Warfare.” *Reuters*, 2018.

Libicki, Martin. “Cyberdeterrence and Cyberwar.” RAND Corporation, 2009.

———. “Norms and Normalization.” In *CyCon US*. Washington: Army Cyber Institute, 2019.

———. “Pulling Punches in Cyberspace.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*, edited by National Research Council (U.S.). Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 123–47. National Academies Press, 2010.

Liff, Adam. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.” *Journal of Strategic Studies* 35, no. 3 (2012): 401–28. https://doi.org/10.1080/01402390.2012.663252.

Lukasik, Stephen J. “A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*, edited by National Research Council (U.S.). Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 99–121. National Academies Press, 2010.

Malagutti, Larissa. “Famous Cyberattacks in Light Og Countries Positions Regarding Principles of International Law,” 2020.

Malagutti, Marcelo. *Dissuasão: Um Olhar Brasileiro*. Brasília: Instituto Vegetius, 2022.

———. “State-Sponsored Cyber-Offences.” *Revista Da Escola de Guerra Naval* 22, no. 2 (2016): 261–90. https://doi.org/10.21544/1809-3191/regn.v22n2p261-290.

———. “Statecraft within Cyberspace.” *Cyber World Magazine*. London, 2017.

Moreira, José de Albuquerque. “Informática: O Mito Política Nacional de Informática.” *Revista de Biblioteconomia de Brasília* 19, no. 1 (1995): 23–50.

Morgan, Patrick. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*, 55–76. National Academies Press, 2010.

Nederlands-MoFA. “Appendix: International Law in Cyberspace,” 2019. https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

Nye, Joseph. “Can China Be Deterred in Cyber Space?” *The Diplomat*, 2016.

———. “Can Cyber Warfare Be Deterred?” *Project Syndicate*, 2015.

———. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (2017): 44–71. https://doi.org/10.1162/ISEC_a_00266.

———. “The Mouse Click That Roared.” *Project Syndicate*, 2013.

Rid, Thomas. *Cyber War Will Not Take Place*. *Journal of Strategic Studies*. Vol. 35. New york: Oxford University Press, USA, 2013. https://doi.org/10.1080/01402390.2011.608939.

———. *Rise of the Machines*. London: Scribe Publications, 2016.

Schelling, Thomas. *Arms and Influence: With a New Preface and Afterword*. Yale University Press, 2008.

Schmitt, Michael. "France's Major Statement on International Law and Cyber: An Assessment." *Just Security*, no. 2 (2019): 2–6.

Singer, J David. "Inter-Nation Influence: A Formal Model." *The American Political Science Review* 57, no. 2 (1963): 420–30. https://doi.org/10.2307/1952832.

Smeets, Max. "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection." *Intelligence and National Security*, 2020. https://doi.org/10.1080/02684527.2020.1729316.

Smeets, Max, and Stefan Soesanto. "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!" *Council on Foreign Affairs*, 2020, 1–6.

Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33, no. 1 (2012): 148–70. https://doi.org/10.1080/13523260.2012.659597.

Stevens, Tim, Kevin O'Brien, Richard Overill, Benedict Wilkinson, Tomas Pildegovičs, and Steve Hill. "UK Active Cyber Defence." London, 2019. https://www.kcl.ac.uk/policy-institute/assets/uk-active-cyber-defence.pdf.

Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (2013): 101–8. https://doi.org/10.1080/01402390.2012.730485.

TED Talks. *Ralph Langner: Cracking Stuxnet, a 21st-Century Cyber Weapon*. TED Talks, 2011.

Toffler, Alvin. *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*. Bantam Books (Transworld Publishers a division of the Random House Group), 1991.

———. *The Third Wave*. William Morrow & Company, 1980.

Toffler, Heidi, and Alvin Toffler. *Revolutionary Wealth: [How It Will Be Created and How It Will Change Our Lives]*. Alfred A. Knopf, 2006.

Tonooka, Eduardo. “Política Nacional de Informática: Vinte Anos de Intervenção Governamental.” *Estudos Econômicos* 22, no. 2 (1992): 273–97.

Tuathail, Gearóid Ó, and John Agnew. “Geopolitics and Discourse. Practical Geopolitical Reasoning in American Foreign Policy.” *Political Geography* 11, no. 2 (1992): 190–204. https://doi.org/10.1016/0962-6298(92)90048-X.

U.S. Government Accountability Office. “The Buy American Act.” U.S. GAO Website, April 5, 1978. https://www.gao.gov/products/105519.

UK-GCHQ. “GCHQ History,” 2016.

US-White House. “Presidential Policy Directive/PPD-20.” Washington, 2012.

———. “Report on Cyber Deterrence,” 2015.

Wright, Jeremy. “Cyber and International Law in the 21st Century.” *Chatham House*. 2018.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York: Crown, 2015.

———. “Everything We Know About Ukraine’s Power Plant Hack.” *Wired*, 2016.

8.6 Capítulo 06 – Os Seis Tipos de Ciberdissuasão

Achten, Nele. “New U.N. Debate on Cybersecurity in the Context of International Security.” *Lawfare*, 2019.

Amin Naves, Guido, and Marcelo Malagutti. “Ciberdefesa (Ou Ciberdefesa).” In *Dicionário de História, Historiadores e Conceitos Militares*, edited by Francisco Carlos Teixeira da Silva, Bruno de Melo Oliveira, Fernando Velôzo Gomes Pedroza, Francisco Eduardo Alves de Almeida, Paulo André Leira Parente, Ricardo Cabral, and Sandro Teixeira Moita, n.d.

Arquilla, John. “From Blitzkrieg to Bitskrieg: The Military Encounter with Computers.” *Communications of the ACM* 54, no. 10 (2011): 58. https://doi.org/10.1145/2001269.2001287.

Austin, Greg. “Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security.” In *Asian Security Conference 2016*, 2016.

Australia-Department of Foreign Affairs and Trade. “Australia’s International Cyber Engagement Strategy.” *Department of Foreign Affairs and Trade*, 2017. https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT AICES_AccPDF.pdf.

Beeker, Kevin R, Robert F Mills, Michael R Grimaila, and Michael W Haas. “Operationally Responsive Cyberspace: A Critical Piece in the Strategic Deterrence Equation.” In *Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*, edited by Adam Lowther. Air University Press, 2013.

Brantly, Aaron. “Entanglement in Cyberspace: Minding the Deterrence Gap.” *Democracy and Security* 16, no. 3 (2020): 210–33. https://doi.org/10.1080/17419166.2020.1773807.

Braw, Elisabeth, and Gary Brown. “Personalised Deterrence of Cyber Aggression.” *RUSI Journal* 165, no. 2 (2020): 48–54. https://doi.org/10.1080/03071847.2020.1740493.

Buchanan, Ben. “Corporate Cybersecurity Is Becoming Geopolitical. Are U.S. Tech Companies Ready?” *Harvard Business Review*, 2018.

———. *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*. C Hurst & Co Publishers, 2017.

Buchanan, Ben, and Thomas Rid. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1–2 (2014): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Bush, George W. “The National Security Strategy United States of America,” no. September (2002): 1–31. http://www.state.gov/documents/organization/63562.pdf.

Carr, Jeffrey. “Cyber Attacks: Why Retaliating against China Is the Wrong Reaction.” *The Diplomat*, August 2015.

Cimpanu, Catalin. “Microsoft, FireEye Confirm SolarWinds Supply Chain Attack.” *ZDNet*, 2020. https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/.

Colatin, Samuele. “A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace.” NATO Cooperative Cyber Defence Centre of Excellence, 2018. https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/.

Columbia, The Grand Jury for the District of. “Annex B App5 Indictment.” Wash, 2018. https://www.justice.gov/file/1080281/download.

CrowdStrike. “2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed.” *2019 Global Threat Report*, 2019. https://crowdstrike.lookbookhq.com/email-global-threat-report-2019/crowdstrike-2019-gtr?ctm_campaign=2019_Global_Threat_Report_EMEA_prospects&ctm_medium=Email&ctm_source=Marketo.

Daskal, Jennifer, Gary Corn, Oona Hathaway, Chantelle Peterson, Cedric Sabbah, and Doug Wilson. “Data and Sovereignty.” *CyCon US*. 2019.

Davis, Paul. “Deterrence, Influence, Cyber Attack and Cyberwar.” *International Law and Politics* 47, no. 327 (2015): 327–55.

Denning, Dorothy. “Rethinking the Cyber Domain and Deterrence.” *Joint Forces Quarterly* 77, no. 2nd Quarter (2015): 8–15.

Devanny, Joe. “The Ethics of Offensive Cyber Operations.” London, 2020.

Elliott, David. “Deterring Strategic Cyberattack.” *IEEE Security & Privacy Magazine* 9, no. 5 (2011): 36–40. https://doi.org/10.1109/msp.2011.24.

Farrell, Henry, and Charles L Glaser. “The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine.” *Journal of Cybersecurity* 3, no. 1 (2017): 7–17. https://doi.org/10.1093/cybsec/tyw015.

Fidler, David. “The UN Secretary-General’s Call for Regulating Cyberwar Raises More Questions Than Answers.” *Council on Foreign Relations Blog*, 2018.

Finnemore, Martha, and Duncan B Hollis. “Constructing Norms for Global Cybersecurity.” *American Journal of International Law* 110, no. 3 (2016): 425–79. https://doi.org/10.1017/s0002930000016894.

France-Ministère des Armées. “International Law Applied to Operations in Cyberspace,” 2019. https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

Freedman, Lawrence. *Deterrence*. London: Polity Press, 2004.

Giles, Keir, and Andrew Monaghan. “Legality in Cyberspace: An Adversary View.” *The Letort Papers*, 2014. http://www.carlisle.army.mil/ssi.

Greenberg, Andy. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” *Wired*, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Grigsby, Alex. “The End of Cyber Norms.” *Survival* 59, no. 6 (2017): 109–22. https://doi.org/10.1080/00396338.2017.1399730.

———. “The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased.” *Council on Foreign Relations*, 2018.

Grimaila, Michael, Robert Mills, and Kevin Beeker. “Applying Deterrence in Cyberspace.” *IO Journal* 1, no. 4 (2010): 21–27.

Hare, Forrest. “The Significance of Attribution to Cyberspace Coercion: A Political Perspective.” In *CyCon 2012*, 1–15. Tallinn: CCDCOE, 2012.

Hayden, Michael. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: The Penguin Press, 2016.

Henriksen, Anders. “The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace.” *Journal of Cybersecurity* 5, no. 1 (2019): 1–9. https://doi.org/10.1093/cybsec/tyy009.

Huang, Zhixiong, and Kubo Mačák. “Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches.” *Chinese Journal of International Law* 16, no. 2 (2017): 271–310. https://doi.org/10.1093/chinesejil/jmx011.

Hutchins, Eric M, Rohan M Amin, and Michael J Cloppert. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” 2010.

Iasiello, Emilio. “Are Cyber Weapons Effective Military Tools?” *Military and Strategic Affairs* 7, no. 1 (2015): 23–40.

———. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security* 7, no. 1 (2014): 54–67. https://doi.org/10.5038/1944-0472.7.1.5.

ICJ. “Statute of the International Court of Justice.” ICJ Website, n.d. https://www.icj-cij.org/en/statute.

Iran-Armed Forces Cyberspace Center. “General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat.” *Nour News*, 2020.

Kaspersky Labs. “O Que é Um Honeypot? Como Os Honeypots Ajudam a Segurança.” Kaspersky website, n.d. https://www.kaspersky.com.br/resource-center/threats/what-is-a-honeypot.

Kaufmann, William. “The Requirements of Deterrence.” Edited by Philip Bobbitt, Lawrence Freedman, and Gregory F Treverton. *US Nuclear*

Strategy. Palgrave Macmillan UK, 1954. https://doi.org/10.1007/978-1-349-19791-0_13.

Kissinger, Henry. *World Order*. New York: Penguin Group (USA), 2014.

Kopp, Carlo. "The Four Strategies of Information Warfare and Their Applications." *IO Journal* 1, no. 4 (2010): 28–33.

Lewis, James. "Cross-Domain Deterrence and Credible Threats," 2010. papers3://publication/uuid/1B60D167-29DA-49E5-825F-06A77C1B17E2.

Libicki, Martin. "Cyberdeterrence and Cyberwar." RAND Corporation, 2009.

———. "Norms and Normalization." In *CyCon US*. Washington: Army Cyber Institute, 2019.

Lynn, William. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (2010).

Mačák, Kubo. "Is the International Law of Cyber Security in Crisis?" In *8th International Conference on Cyber Conflict*, 2016-Augus:127–39. Tallinn: NATO/CCDCOE, 2016. https://doi.org/10.1109/CYCON.2016.7529431.

Malagutti, Marcelo. *Dissuasão: Um Olhar Brasileiro*. Brasília: Instituto Vegetius, 2022.

———. "State-Sponsored Cyber-Offences." *Revista Da Escola de Guerra Naval* 22, no. 2 (2016): 261–90. https://doi.org/10.21544/1809-3191/regn.v22n2p261-290.

———. "Why Should Nations Pursue Their Software Power ?," 2016.

Martin, Ciaran. "Cyber-Weapons Are Called Viruses for a Reason : Statecraft and Security in the Digital Age." 2020.

Medeiros, Breno, and Luiz Goldoni. "The Fundamental Conceptual Trinity of Cyberspace." *Contexto Internacional* 42, no. 1 (2020): 31–54. https://doi.org/10.1590/s0102-8529.2019420100002.

Nederlands-MoFA. "Appendix: International Law in Cyberspace," 2019. https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

New Zealand. “The Application of International Law to State Activity in Cyberspace,” 2020. https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il.

Nye, Joseph. “Can China Be Deterred in Cyber Space?” *The Diplomat*, 2016.

———. “Cyber Power,” 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

———. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (2017): 44–71. https://doi.org/10.1162/ISEC_a_00266.

———. “How Will New Cybersecurity Norms Develop?” *Project Syndicate*, 2018.

Pereira, Antônio Celso Alves. “A Legítima Defesa No Direito Internacional Contemporâneo.” *Revista Interdisciplinar de Direito* 7, no. 1 (2010): 21–36.

Schelling, Thomas. *Arms and Influence: With a New Preface and Afterword*. Yale University Press, 2008.

Schmidt, Michael, and Nicole Perlroth. “U.S. Charges Russian Intelligence Officers in Major Cyberattacks.” *The New York Times*, 2020.

Schmitt, Michael. *Tallinn Manual 2.0 on the International Law Applicable To Cyber Operations*. Edited by NATO/CCDCOE. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2017.

———. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Edited by NATO/CCDCOE. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013. https://doi.org/10.1017/cbo9781139169288.

Schmitt, Michael, and Liis Vihul. “The Nature of International Law Cyber Norms.” *CCDCOE Tallinn Papers*, no. 5 (2014). https://doi.org/10.2307/1952804.

Sklerov, Matthew. “Responding to International Cyber Attacks.” In *Inside Cyber Warfare: Mapping the Cyber Underworld*, edited by Jeffrey Carr, 46–62. Sebastopol, CA: O’Reilly, 2010.

Snyder, Glenn. “Deterrence by Denial and Punishment,” 1959.

Sterling, Bruce. “Flame/Stuxnet/Duqu Are Attacking Kaspersky.” *Wired*, 2015.

Stevens, Tim. “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace.” *Contemporary Security Policy* 33, no. 1 (2012): 148–70. https://doi.org/10.1080/13523260.2012.659597.

UK-MoD. “Cyber Primer.” *Cyber Primer*, 2016.

US-White House. “Report on Cyber Deterrence,” 2015.

Vegetius, Flavius Renatus. *De Re Militari*, 1767.

Marcelo Malagutti é Pesquisador Sênior do Instituto Vegetius. É Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME) com um ano como Doutorando Visitante no King's College London (Reino Unido); Mestre em Estudos de Guerra pelo King's College London; Diplomado no Curso de Altos Estudos em Política e Estratégia pela Escola Superior de Guerra (ESG); MBA em Estratégia Corporativa pela Fundação Getúlio Vargas (FGV); Bacharel em Ciência da Computação pela Universidade de Brasília (UnB); Agraciado com a Medalha do Pacificador e a Medalha Exército Brasileiro; Empresário do Setor de Software; Membro do King's College Cyber Security Research Group; Membro do King's College Wargaming Network.

Pode o "Software Power" (Poder de Software) ser uma ferramenta de coação e de dissuasão entre estados nacionais? Esta é a questão respondida neste livro, escrito com um enfoque didático voltado a explicar questões estratégicas da ciberdefesa e cibersegurança para pessoas que não necessariamente tenham conhecimento de informática, computação nem tecnologia da informação. Ele apresenta os conceitos fundamentais relacionados a ciberofensas estatais e "ciberguerra" como instrumentos de coação interestatal, versa sobre a cultura estratégica brasileira e sua influência na preparação do país para dissuadir tais ameaças e apresenta sugestões de elevação das cibercapacidades brasileiras, implementáveis rapidamente e de baixo custo relativo.

O Instituto Vegetius é uma instituição brasileira, de caráter filantrópico, sem finalidades lucrativas e sem qualquer vinculação política ou partidária, que atua na área social mediante a realização de pesquisas, estudos, análises e ações voltados a auxiliar na melhoria de políticas públicas e tomada de decisão e no engajamento da sociedade nos temas de defesa nacional, segurança nacional e internacional, guerra e a paz, relações entre forças armadas e sociedade, ciência e tecnologia no âmbito da defesa e segurança nacionais e internacionais, geopolítica e relações internacionais, planejamento, estratégia, estudos estratégicos e ciências militares em geral.

As publicações do Instituto Vegetius não necessariamente refletem as opiniões de seus clientes e patrocinadores.

INSTITVTO VEGETIVS

www.vegetius.org.br

ISBN: 978-65-997420-1-9
CBL
9 786599 742019