OASIS
OBSERVATORIO DE ANÁLISIS DE LOS SISTEMAS INTERNACIONALES

Oasis
ISSN: 2346-2132
ISSN: 1657-7558
Universidad Externado de Colombia

Araújo-Lisboa, Cícero; Ziebell-de Oliveira, Guilherme
O conceito de dissuasão cibernética: relevância e possibilidades
Oasis, núm. 35, 2022, pp. 53-78
Universidad Externado de Colombia

DOI: https://doi.org/10.18601/16577558.n35.04

Disponível em: https://www.redalyc.org/articulo.oa?id=53172100004

O conceito de dissuasão cibernética: relevância e possibilidades

Cícero Araújo Lisboa[*]
Guilherme Ziebell de Oliveira[**]

RESUMO

Este artigo busca discutir a possibilidade de aplicação do conceito de dissuasão ao ambiente cibernético. Dada a sua crescente importância, o ciberespaço ocupa uma dimensão central nas preocupações estratégicas de qualquer nação. Diante da possibilidade de conflitos cibernéticos, a reflexão sobre o conceito de dissuasão cibernética, bem como sua relevância, é essencial. Assim, o trabalho busca discutir o conceito, considerando suas aplicações e limitações, bem como suas principais características, avaliando suas semelhanças e diferenças em relação ao conceito de dissuasão convencional. Após uma discussão sobre o conceito de dissuasão e suas particularidades, ele apresenta uma análise da cibersegurança, com atenção especial para a discussão das ameaças cibernéticas. Por fim, discute a aplicação do conceito de dissuasão no campo da cibersegurança, demonstrando sua aplicabilidade e destacando suas principais potencialidades e limites.

Palavras-chave: dissuasão cibernética; dissuasão convencional; segurança cibernética; segurança internacional.

EL CONCEPTO DE DISUASIÓN CIBERNÉTICA: PERTINENCIA Y POSIBILIDADES

RESUMEN

Este artículo pretende discutir la posibilidad de aplicar el concepto de disuasión en el am-

[*] Especialista em Gestão da Segurança e Defesa Cibernéticas (UFRGS). Mestrando do Programa de Pós-Graduação em Estudos Estratégicos Internacionais (PPGEEI) Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre (Brasil). [cicero.lisboa@ufrgs.br]; [https://orcid.org/0000-0003-4400-9536].

[**] Doutor em Ciência Política (PPGPOL/UFRGS). Professor do Programa de Pós-Graduação em Estudos Estratégicos Internacionais (PPGEEI) Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre (Brasil). [guilherme.ziebell@ufrgs.br]; [https://orcid.org/0000-0002-0118-6279].

Recibido: 17 de abril de 2021 / Modificado: 2 de julio de 2021 / Aceptado: 6 de julio de 2021.

Para citar este artículo:

Araújo Lisboa, C. y Ziebell de Oliveira, G. (2022). O conceito de dissuasão cibernética: relevância e possibilidades. *OASIS,* 35, pp. 53-78

DOI: https://doi.org/10.18601/16577558.n35.04

biente cibernético. En vista de su creciente importancia, el ciberespacio ocupa una dimensión central en las preocupaciones estratégicas de cualquier nación. Ante la posibilidad de conflictos cibernéticos, la reflexión sobre el concepto de disuasión cibernética, así como sobre su relevancia, es fundamental. De esta forma, el trabajo busca discutir el concepto, considerando sus aplicaciones y limitaciones, como también sus principales características, evaluando sus similitudes y diferencias con relación al concepto de disuasión convencional. Tras una discusión sobre el concepto de disuasión y sus particularidades, presenta un análisis de la ciberseguridad, dando especial atención a la discusión de las ciberamenazas. Finalmente, discute la aplicación del concepto de disuasión en el ámbito de la ciberseguridad, demostrando su aplicabilidad y destacando sus principales potenciales y límites.

Palabras-clave: disuasión cibernética, disuasión convencional, seguridad cibernética, seguridad internacional.

THE CONCEPT OF CYBER DISSUASION: RELEVANCE AND POSSIBILITIES

ABSTRACT

This article aims to discuss the applicability of the concept of deterrence to the cyberspace. In view of its growing importance, cyberspace occupies a central dimension in the strategic concerns of any nation. Given the possibility of cybernetic conflicts, reflection on the concept of cyber deterrence, as well as its relevance, is essential. Thus, this article seeks to discuss the concept, considering its applications and limitations, as well as its main characteristics, evaluating its similarities and differences in relation to the concept of conventional deterrence. After a discussion on the concept of deterrence and its particularities, it presents an analysis of cybersecurity, paying special attention to the discussion of cyber threats. Finally, it discusses the application of the concept of deterrence in the field of cybersecurity, demonstrating its applicability and highlighting its main potentials and limitations.

Keywords: cyber deterrence, conventional deterrence, cyber security, international security.

1 INTRODUÇÃO

Em maio de 2019, em mais um capítulo de violência entre Israel e Palestina, na faixa de Gaza, 25 palestinos e 4 israelenses foram mortos em um final de semana, durante um bombardeio. Após décadas de conflito, isso não seria, por si só, uma surpresa. Entretanto, um aspecto chamou atenção dos especialistas em segurança e defesa: pela primeira vez as Forças Armadas de Israel haviam bombardeado um prédio que supostamente serviria de base para um grupo de *hackers* do Hamas (Newman, 2019). Por meio de seu perfil na rede social *Twitter*, as Forças Armadas de Israel (IDF) afirmaram que haviam frustrado "uma tentativa de ofensiva cibernética do Hamas contra alvos israelenses. Após nossa operação de defesa cibernética bem-sucedida, visamos um prédio

onde o Hamas operava no ciberespaço. HamasCyberHQ.exe foi removido" (IDF, 2019, n.p., tradução nossa).

Considerado por especialistas em segurança e defesa como o primeiro ataque físico disparado como resposta a ataques digitais, tal fato, contudo, não é surpreendente (Doffman, 2019). Desde 2011, a estratégia nacional de segurança cibernética dos Estados Unidos considera a possibilidade de uma resposta cinética contra ataques realizados através do ciberespaço (The White House, 2011; 2018). Tal questão se mostra de grande relevância para o país, não apenas porque os Estados Unidos são cada vez mais dependentes do ciberespaço para os fluxos de bens e serviços, para o suporte ao controle de suas infraestruturas críticas –como eletricidade, distribuição de água, sistema financeiro, transporte e comunicação–, e para o comando e controle de sistemas militares, mas também porque tal dependência é acompanhada por um aumento simultâneo da quantidade e da capacidade de atividades maliciosas no ciberespaço desenvolvidas por outros atores –estatais ou não-estatais (Nye, 2016).

Através do ciberespaço, hoje é possível controlar infraestruturas críticas, gerir sistemas financeiros, armazenar propriedade intelectual, prover serviços de governo eletrônico, entre outros. Todas essas possibilidades de uso transformaram o ciberespaço em um ambiente estratégico para os governos, os negócios e as sociedades (Ten, Manimaran & Liu, 2010). Entretanto, existem, também, muitas ameaças no ciberespaço. Em 2019, o Fórum Econômico Mundial elencou os ataques cibernéticos entre os cinco maiores riscos que a humanidade enfrentaria naquele ano (Myers & Whiting, 2019). De acordo com o Relatório Anual Oficial de Crimes Cibernéticos de 2019, da *Cybersecurity Ventures*,[1] o crime cibernético é a maior ameaça para todas as empresas no mundo, e um dos maiores problemas que a humanidade enfrenta. O relatório estima que o cibercrime custará ao mundo mais de US$ 6 trilhões por ano até o final de 2021, ante US$ 3 trilhões em 2015 (Ventures, 2020).

Casos de ataque à soberania dos países também representam uma ameaça no ciberespaço. Um dos eventos mais conhecidos foi o da sabotagem das instalações nucleares do Irã, em 2010, através do *worm*[2] de computador *Stuxnet*, que causou a destruição de grande parte da planta de enriquecimento de urânio daquele país, supostamente de autoria dos Estados Unidos e de Israel (Singer & Friedman, 2014; Zetter, 2017). Outro caso importante ocorreu em 2007, na Estônia, quando, após divergências entre o governo do país e o governo da Rússia sobre a remoção de um memorial da Segunda Guerra, a Estônia passou a receber ataques cibernéticos em massa, que eram destinados ao governo, aos bancos e à imprensa. Para fazer frente aos ataques, o governo estoniano

[1] A *Cybersecurity Ventures* é líder mundial em pesquisas para o ciberespaço.
[2] Semelhante a um vírus de computador, podendo prejudicar usuários e sistemas de diversas formas.

precisou desativar o acesso de endereços IP[3] externos, e o país levou meses para se recuperar totalmente dos ataques sofridos (Clarke & Knake, 2011).

Há, ainda, outros casos que podem ser citados. Especula-se que em 2007 Israel tenha utilizado armas cibernéticas para impedir que a Força Aérea Síria percebesse o avanço de aviões israelenses, que passaram sem ser detectados pelos radares sírios no ataque aéreo realizado ao país árabe em setembro daquele ano (Singer & Friedman, 2014). Em 2008, a Geórgia, durante o conflito que se desenrolou com a Rússia, sofreu ataques de negação de serviço[4] que paralisaram sua *Internet*, limitando a capacidade do governo de se comunicar com a população e o mundo, ao mesmo tempo em que as forças russas cruzavam sua fronteira (Clarke & Knake, 2011). Também pode-se citar o Brasil, que foi alvo de um programa de vigilância mantido pelos Estados Unidos, que monitorava *e-mails* e ligações telefônicas do governo brasileiro. Este fato foi revelado por Edward Snowden, em 2013, e provocou mal-estar diplomático entre os governos dos dois países (Ferraço, 2014).

Com os Estados cada vez mais incorporando capacidades de segurança e defesa cibernéticas, tem havido um incremento na busca por capacitar suas organizações para promover a proteção de seus ativos de informação mais valiosos e de suas infraestruturas críticas. Desta forma, a partir do momento em que dispositivos de controle, sejam industriais ou militares, começam a utilizar funcionalidades definidas por *software*, tornam-se vulneráveis às ameaças do ciberespaço. Assim, medidas de segurança cibernética tornaram-se necessárias para a proteção destes, e, até mesmo, para desenvolver ações de planejamento militar contra ataques, conforme o nível de criticidade dos ativos envolvidos –uma vez que todos os ativos críticos apresentam algum grau de vulnerabilidade a ameaças, mesmo que não evidente.

A existência de eventos que misturam ações militares e de inteligência é fundamental para que muitos pesquisadores considerem que nos aproximamos, cada vez mais, a um cenário de potencial eclosão de guerras cibernéticas em nível global (Nye, 2016). É justamente frente à possibilidade de existência de conflitos dessa natureza que a reflexão a respeito da aplicabilidade do conceito de dissuasão ao âmbito cibernético, bem como de sua viabilidade e relevância, se impõe, trazendo consigo um questionamento acerca da possibilidade de um país dissuadir outros Estados ou grupos não-estatais no âmbito do ciberespaço. Para alguns pesquisadores, o conceito de dissuasão é inseparável da ideia de ameaça de punição retaliatória –ou seja, a teoria de dissuasão clássica repousa em dois mecanismos principais,

[3] Rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de *Internet* para comunicação.

[4] A Negação de Serviço ocorre quando *sites* são repentinamente submetidos a uma grande quantidade de acessos, sobrecarregando assim os recursos computacionais dos servidores-alvo.

uma ameaça crível de punição por uma ação e a negação de ganhos de uma dada ação. No livro *Arms and Influence*, Schelling (1966) refere-se ao poder de ferir como um dos atributos mais relevantes da força militar, já que a expectativa de sofrimento pode motivar as potenciais vítimas a querer evitar a dor ou a tentar evitar perder algo.

Existem, no entanto, muitas dúvidas sobre a possibilidade de uma dissuasão no âmbito cibernético imprimir nos adversários, de forma efetiva, a mesma linguagem utilizada na dissuasão convencional. Autores como Geers (2011) e Lewis (2009), por exemplo, consideram que as especificidades do mundo cibernético fazem com que ele seja incompatível com a noção de dissuasão. Tendo isso em conta, o presente trabalho busca responder à seguinte pergunta: o conceito de dissuasão –tradicionalmente aplicado nas discussões de Relações Internacionais às esferas nuclear e militar tradicional –pode ser aplicado também ao âmbito cibernético? Nesse contexto, o trabalho busca, partindo de elementos da perspectiva teórica realista e agregando elementos de aportes teóricos distintos, discutir a aplicabilidade do conceito de dissuasão ao âmbito cibernético. Para tanto, considera suas possíveis aplicações e limitações,[5] bem como suas características principais, além de avaliar similaridades e diferenças em relação às noções convencionais de dissuasão.

Para isso, a pesquisa adota metodologia qualitativa, apoiando-se em uma revisão bibliográfica (sobretudo de livros e artigos centrados nas discussões sobre o conceito de dissuasão e sobre segurança cibernética) e documental (dentre os quais destacam-se as estratégias de segurança e defesa cibernéticas, além de convenções sobre o tema), e em uma abordagem interpretativa e privilegiando, em grande medida, um enfoque centrado nas perspectivas e doutrinas de atores como o Brasil e os EUA. Sendo assim, e de forma a atingir os objetivos propostos, o artigo está estruturado em três seções, além desta introdução e da seção de conclusão. Na primeira seção é apresentada, a partir de uma revisão de literatura, uma contextualização dos diversos elementos que compõem a noção de dissuasão convencional, sua definição e características, de forma a detectar quais são os elementos comumente identificados como característicos da dissuasão. A segunda seção, por sua vez, apresenta uma discussão a respeito do conceito de segurança cibernética, fazendo uma análise em relação à segurança da informação e da segurança dos ativos de tecnologia de informação e comunicação. Por fim, na terceira seção, é apresentada uma análise da possibilidade de aplicação do conceito de dissuasão no âmbito da segurança cibernética. Nesse sentido, busca-se, a partir de uma análise interpretativa, avaliar se os elementos que

[5] A reflexão considera três possíveis situações que se enquadram na noção de dissuasão cibernética: i) ameaças físicas visando dissuadir ações no ciberespaço; ii) ameaça no ciberespaço visando dissuadir ações no mundo físico; iii) ameaça no ciberespaço visando dissuadir ações no ciberespaço.

compõem a noção de dissuasão convencional - identificados na primeira seção - são também aplicáveis ao ambiente cibernético - e, em caso contrário, quais são as limitações existentes a essa aplicação. A partir dessa reflexão, pretende-se demonstrar que, a despeito da existência de limitações e/ou desafios à aplicação dos diversos componentes do conceito de dissuasão ao ambiente cibernético - os quais resultam justamente das especificidades do ciberespaço -, é possível aplicar o conceito de dissuasão ao ambiente cibernético.

2. O CONCEITO DE DISSUASÃO

O conceito de dissuasão, em sua essência, pode ser entendido como a decisão de um ator de não realizar uma determinada ação contra um segundo ator, a partir da percepção de que os potenciais custos e riscos envolvidos em tal ação não compensam os eventuais benefícios esperados (Mearsheimer, 1981). Ainda que as discussões sobre a questão remontem ao menos ao século V a.C., no contexto da Guerra do Peloponeso,[6] sua relevância contemporânea para as Relações Internacionais começou a se desenhar nos anos iniciais do século XX (Jervis, 1979). Os desenvolvimentos tecnológicos do período, especialmente a possibilidade de realização de ataques aéreos, foram fundamentais para que passassem a ser feitas reflexões mais aprofundadas a respeito da ideia de dissuasão (Muller, 2004). Foi, contudo, a partir da Segunda Guerra Mundial, marcada por um aumento significativo da capacidade destrutiva dos armamentos –especialmente a partir do emprego dos artefatos nucleares estadunidenses em Hiroshima e Nagasaki, no Japão–, que a dissuasão passou a ocupar um espaço de destaque nas discussões do campo das Relações Internacionais - sobretudo entre os teóricos da corrente de pensamento realista (Morgan, 2003).

Nesse contexto, imediatamente após o fim do conflito mundial, autores como Bernard Brodie (1946) e Arnold Wolfers (1946) passaram a elaborar discussões a respeito das implicações dos armamentos nucleares para a dissuasão. Em linhas gerais, para tais autores, a existência dos artefatos nucleares havia alterado fundamentalmente a natureza da guerra, impondo, assim, uma revolução estratégica, uma vez que, se antes o objetivo era vencer os conflitos, a partir de então o objetivo passava a ser evitar que eles ocorressem (Putten, Meijnders, & Rood, 2015). Tal transformação resultaria justamente da possibilidade de destruição total representada pelo eventual uso dos artefatos nucleares, bem como da incapacidade de defesa daqueles Estados que não detivessem tais armamentos (Brodie, 1946; Jervis, 1979).

A partir da década de 1950, uma nova onda de estudos sobre dissuasão começou a tomar forma. Buscando incorporar maior "rigor científico" e capacidade de abstração às reflexões, diversos autores passaram a incor-

[6] A discussão sobre a ameaça do uso da violência em resposta às ações adversárias aparece na célebre obra de Tucídides sobre a Guerra do Peloponeso (Thucydides, 2009).

porar elementos de Teoria dos Jogos às suas discussões, especialmente o chamado "*Chicken game*"[7] (Brantly, 2018). Nesse sentido, autores como Brodie (1959), Wholstetter (1959), Schelling (1960; 1966) e Snyder (1961) procuraram demonstrar a importância da noção de racionalidade dos atores para a ideia de dissuasão. A estratégia, assim, passava a ser tratada como um processo de barganha, no qual os adversários buscariam, por meio de ameaças, promessas e ações, influenciar as expectativas e intenções uns dos outros. Ela seria, portanto, a arte da coerção, da intimidação e, também, da dissuasão (Schelling, 1966).

A despeito das contribuições aportadas pelas reflexões desta segunda onda, muitas foram as críticas ao seu desenvolvimento, o que levou ao surgimento de uma nova onda de estudos, a qual incorporou, entre outros, elementos da Psicologia Cognitiva e de estudos comportamentais

(Karpavičiūtė, 2019). Autores como Allison (1971), George e Smoke (1974), Steinbruner (1976), Janis (1982) e Jervis, Lebow e Stein (1985), entre outros, a partir de diferentes perspectivas e abordagens, elaboraram discussões que questionavam não apenas a falta de evidências empíricas e o forte recurso à dedução nas análises de dissuasão, mas também os próprios pressupostos de racionalidade e sua fragilidade nos processos de tomada de decisão. Os estudos elaborados nesse contexto, os quais buscavam maior suporte em evidências empíricas, demonstraram a necessidade de revisão das Teorias de Dissuasão em certos elementos (como definição de riscos, recompensas, probabilidades, erros de percepção e burocracia e política doméstica), procurando desenvolver novas soluções para todos eles (Jervis, 1979; Walt, 1991).

Autores como Knopf (2010), Lupovici (2010), Putten, Meijnders e Rood (2015) e Karpavičiūtė (2019)[8] identificam ainda a existência de uma quarta onda de estudos de dissuasão. Enquanto as três primeiras tinham como motivador principal e elemento central das discussões a questão dos armamentos nucleares –e as inúmeras possíveis consequências de sua existência –, a nova vertente teria se estruturado a partir do fim da Guerra Fria, sobretudo diante da noção de emergência de "novas" ameaças, tendo ganhado força especialmente depois dos atentados de 11 de setembro de 2001 aos Estados Unidos (Knopf, 2010).

Assim, a nova onda se distinguiria das anteriores, principalmente, por duas características. Primeiro, por seu enfoque, não mais centrado exclusivamente nos armamentos

[7] Trata-se de um jogo simétrico, em que os dois competidores, ao se confrontarem, têm como opções continuar ou desistir. Se nenhum dos dois desistir, ambos perdem tudo. Se apenas um desistir, este sai como o único perdedor –ainda que sem uma derrota total.

[8] Karpavičiūtė (2019) ainda identifica uma quinta onda, que teria início a partir dos anos 2010, centrando-se, a partir da compatibilização de elementos teóricos das quatro primeiras ondas, em discussões sobre dissuasão multidimensional e sobre os impactos tecnológicos e o papel da inteligência artificial na dissuasão. A despeito da segmentação proposta pela autora, para este estudo consideramos que tais discussões, dadas suas naturezas, são pertinentes, ainda, a uma quarta onda de estudos sobre dissuasão.

nucleares e em ameaças tradicionais, mas incorporando discussões a respeito de uma gama muito mais ampla de ameaças, como violência perpetrada por atores não-estatais e guerras assimétricas (Putten, Meijnders & Rood, 2015). Segundo, por seu caráter, que teria uma natureza interpretativa, dedicando grande relevância para o contexto intersubjetivo da dissuasão, entendido como sendo fundamental para a construção da compreensão dos atores nela envolvidos a respeito de seu significado (Lupovici, 2010). Nesse sentido, como destacado por Gray (1990; 1999), a dissuasão se estabeleceria não necessariamente (e tampouco de forma exclusiva) a partir das capacidades concretas do Estado dissuasor, mas sim a partir da percepção, do Estado dissuadido, a respeito dessa capacidade e de suas implicações.

A despeito da existência de inúmeras (e relevantes) distinções entre as quatro ondas de estudos de dissuasão[9] –especialmente no que diz respeito aos diferentes enfoques por elas adotados –, em linhas gerais é possível identificar a existência de sete componentes, que atuam de forma conjunta e inter-relacionada e que são fundamentais para a dissuasão - independente do enfoque adotado (Goodman, 2010; Wilner, 2017; McKenzie, 2017). O primeiro é a existência de um determinado interesse, o qual o agente dissuasor busca proteger. O segundo componente é a declaração dissuasória, que tem por objetivo apresentar, de forma clara e compreensível (e aceita) pelos demais agentes, o interesse que o ator busca proteger, bem como seu compromisso político com sua proteção e as consequências a serem impostas aos demais atores caso ataquem tal interesse –as ações de dissuasão (Goodman, 2010; McKenzie, 2017).

As ações de dissuasão são o terceiro componente, e podem ser de dois tipos: medidas de punição ou de negação (Snyder, 1961; Gray, 1990; Libicki, 2009). Medidas de punição compõe o aspecto ofensivo da dissuasão, sendo aquelas em que o ator dissuasor ameaça retaliar um eventual agressor caso ele realize uma ação indesejada –ou seja, a tentativa de dissuasão se constrói a partir da ameaça de impor custos ao eventual agressor (George & Smoke, 1974). Por outro lado, as medidas de negação são o aspecto defensivo da dissuasão, e dizem respeito à capacidade de demover um potencial agressor de sua intenção de atacar por meio da redução dos eventuais benefícios a serem conquistados com tal ataque (Knopf, 2010). Este tipo de dissuasão ocorreria em casos em que o ator dissuasor demonstrasse resiliência –sendo esta entendida como a capacidade de mitigar efeitos de um eventual ataque (dissuasão por prevenção) e/ou de se recuperar rapidamente após ser atingido (dissuasão por futilidade). Assim, como destaca Wilner (2017, p. 310,

[9] Cumpre ressalvar que a ideia de distintas ondas de estudos sobre dissuasão utilizada aqui em grande medida reflete os desenvolvimentos teóricos sobre o tema produzidos nos (e/ou que partem da perspectiva dos) EUA - sendo centradas, portanto, sobretudo na noção de dissuasão nuclear. Assim sendo, tal divisão não leva em consideração os desenvolvimentos da literatura focada na dissuasão convencional, em geral elaborada a partir do enfoque na realidade de outros países, destituídos de armamentos nucleares.

tradução nossa) "[e]m suma, dissuasão por punição [...] ameaça causar danos, adicionando custos a determinados comportamentos; a dissuasão por negação [...] ameaça o fracasso, subtraindo benefícios de determinado comportamento".

O quarto componente é a credibilidade (entendida como a plausibilidade e expectativa de sucesso das eventuais ações de dissuasão expressas na declaração dissuasória), o quinto é a confiança (a garantia de que não haverá punições caso não haja atentados contra o interesse que está sendo protegido) e o sexto é o medo (do ator dissuadido em relação às ações de dissuasão) (Lupovici, 2010; Wilner, 2020). Por fim, o sétimo componente é o cálculo de custo-benefício, que envolve todos os componentes anteriores e que, em última instância, é o que determina o comportamento do ator que se busca dissuadir (Mearsheimer, 1981).

3. SEGURANÇA E DEFESA CIBERNÉTICAS

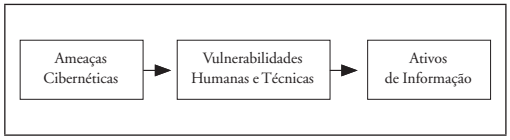
Para tratar sobre segurança cibernética, é necessário conhecer o conceito de segurança da informação, que é definido pela norma internacional ISO/IEC 27000:2018 como a preservação da confidencialidade, integridade e disponibilidade da informação (CID) (ISO, 2018). Diante disso, a informação pode ter muitas formas, armazenada em papel ou meio eletrônico, e podendo ser transmitida através da voz, do papel e eletronicamente através dos meios digitais –como filmes, músicas, entre outros (ISO, 2018). Em uma visão mais ampla, pode-se definir a segurança da informação como uma área do conhecimento que estuda a proteção dos ativos[10] de informação contra acessos não autorizados, alterações indevidas e sua indisponibilidade. Dessa forma, a área de conhecimento trata de criar regras que devem incidir sobre todo o ciclo de vida da informação (manuseio, armazenamento, transporte e descarte), buscando identificar ameaças, vulnerabilidades e seus possíveis controles (Sêmola, 2014).

As ameaças são agentes ou condições que afetam as informações e seus ativos por meio da exploração de vulnerabilidades, causando a perda dos atributos de confidencialidade, integridade e disponibilidade, acarretando impactos nos negócios/processos de uma organização. As vulnerabilidades, por outro lado, são fragilidades presentes em ativos de informação que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação. Vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, ou seja, precisam de um agente causador, que são as ameaças (Sêmola, 2014). Um exemplo disso são os erros de codificação ou a configuração incorreta de sistemas, aplicativos ou equipamentos, que, consequentemente, podem levar a ameaças, como acessos indevidos e vazamentos de dados, entre outros. A Figura 1, abaixo, sintetiza as relações existentes entre ameaças,

[10] Considera-se um ativo tudo aquilo que tem valor para um indivíduo, uma organização ou um governo.

vulnerabilidades e ativos de informação, conforme discutidas acima.

Figura 1
Relação entre ameaças, vulnerabilidades e ativos de informação



Fonte: Elaborado pelos autores

A segurança cibernética se destina à proteção do ciberespaço, e os recursos que mantêm esse ambiente são oriundos de ativos de tecnologia de informação e comunicação (TIC), formados através de um ambiente de natureza híbrida - *hardware* e *software* - e interligados por inúmeras redes de computadores. O ciberespaço é definido como o "[a]mbiente complexo resultante da interação de pessoas, *software* e serviços na *Internet*, suportado por instrumentos físicos de tecnologia da informação e comunicação (TIC) e redes conectadas e distribuídas pelo mundo inteiro" (ABNT, 2015, p. 9).

No entanto, quando se estuda o ciberespaço, existem questões de segurança não atendidas pela atual segurança da informação, como a de *Internet*, a de redes e as melhores práticas recomendadas de segurança de TIC, bem como os vácuos entre esses domínios e a falha de comunicação entre organizações e provedores no ciberespaço (ABNT, 2015). Dessa forma, a segurança cibernética se baseia na segurança da informação, na segurança da *Internet* e na segurança de TIC, como blocos de construção fundamentais, mas sua definição considera que a proteção do ciberespaço deve levar em conta aspectos físicos, sociais, financeiros, políticos, emocionais, profissionais, psicológicos, educacionais ou outros tipos ou consequências de falhas, danos, erros, acidentes, prejuízos ou quaisquer eventos considerados indesejáveis neste ambiente (ABNT, 2015). As ações de segurança cibernética visam proteger a sociedade, os governos e as empresas dos novos desafios do ciberespaço, tais como o *cyberbullying,* a espionagem cibernética, o ciberterrorismo e o ataque cibernético entre países (Von Solms & Van Niekerk, 2013).

Os exemplos citados demonstram o quão heterogêneas são as ameaças do ciberespaço. Devido a isso, alguns países, como Austrália (Australian Government, 2020), Colômbia (República de Colombia, 2016), Espanha (Gobierno de España, 2019) e Estados Unidos (The White House, 2018), desenvolveram estratégias de segurança cibernética, alinhadas com suas estratégias nacionais de segurança, para promover a proteção da privacidade, da sociedade, dos negócios, da propriedade intelectual e das suas infraestruturas críticas. Essas estratégias propõem uma série de ações, como conscientização da população, educação de profissionais, políticas de desenvolvimento de uma indústria *ciber* e o estabelecimento de órgãos responsáveis –em suma, estabelecem os objetivos para que uma nação tenha um ciberespaço mais seguro.

Isto posto, torna-se difícil enquadrar as ações de interrupção, sabotagem e crime cibernético na mesma categoria de ações previstas numa estratégia de segurança cibernética, como o que ocorreu contra a Estônia, por exemplo. Essas ações ofensivas recaem sobre a responsa-

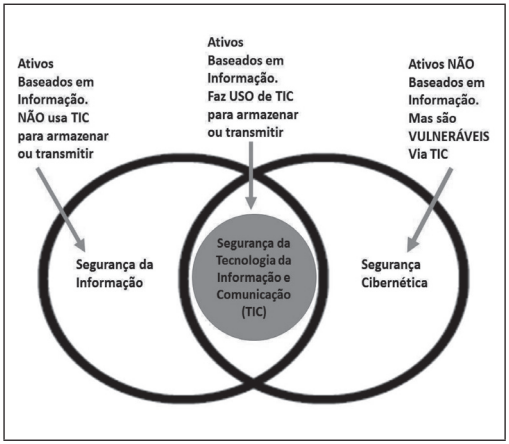
bilidade das forças armadas, compreendendo, assim, a defesa cibernética. A Doutrina Militar de Defesa Cibernética do Brasil a define como

> Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (Brasil, 2014, p. 18).

Segundo Villa e Reis (2006), o conceito de segurança cibernética está mais ligado a questões defensivas, fazendo referência ao combate e à prevenção dos chamados crimes cibernéticos na esfera pública –ou seja, no nível político. Já as ações defensivas, ofensivas e exploratórias realizadas no ciberespaço, dentro de um contexto de planejamento militar, são coordenadas por um órgão militar. Assim, considerando-se os aspectos táticos e operacionais do ciberespaço, são as forças armadas que têm a responsabilidade de aplicar a estratégia, com a finalidade de prevenir ou responder em caso de ataques cibernéticos contra a soberania nacional. Muitos países já possuem sua força *ciber* formalizada, como o Brasil (CDCiber) e os Estados Unidos (USCYBERCOM).

Por fim, com base no tipo de ativo e na necessidade do uso, ou não, de TIC, é possível dizer que a segurança da informação é baseada em qualquer tipo de ativo de informação, não precisando, necessariamente, estar armazenado em ativos de TIC. No caso da segurança de TIC, os ativos de informação são baseados em TIC para transmissão e armazenamento (computadores, redes, *pendrives*, *smartphones*, etc.). Na segurança cibernética, por outro lado, os ativos não precisam ser baseados em informação, sendo, contudo, vulneráveis através de recursos de TIC (pessoas, infraestruturas críticas, etc.). A Figura 2 demonstra, de forma sintetizada, a intersecção e/ou correlação entre a segurança da informação, a segurança de TIC e a segurança cibernética, e suas dependências em relação aos ativos de informação.

Figura 2
Correlação entre Segurança da Informação, Segurança de TIC e Segurança Cibernética



Fonte: Adaptada pelos autores a partir de Von Solms e Van Niekerk (2013, p. 101).

4. APLICAÇÃO DO CONCEITO DE DISSUASÃO NO ÂMBITO DA SEGURANÇA CIBERNÉTICA, SEUS DESAFIOS E LIMITAÇÕES

A dissuasão, conforme apresentada anteriormente, em sua essência, significa convencer um oponente a não iniciar uma ação específica,

porque os benefícios percebidos não justificam os custos e riscos potenciais. Embora seu livro *The Theory and Practice of Conventional Deterrence* tivesse como foco de estudo a prevenção da guerra, Mearsheimer (1981) aponta que não apenas considerações militares contribuem para a dissuasão, mas também outros elementos, como as ações de aliados, o Direito Internacional e fatores econômicos, exercem influência sobre uma nação que pretende empreender uma ação militar.

Em seu livro, *Cyberdeterrence and Cyberwar*, Libicki (2009) descreve as opções de dissuasão por negação (capacidade de resistir aos/frustrar os ataques) e dissuasão por punição (a ameaça de retaliar). A partir dessas nomenclaturas, o autor estabelece uma distinção, do ponto de vista cibernético, entre dissuasão cibernética passiva (negação) e ativa (punição). A dissuasão passiva seria responsável por implementar as ações de segurança da informação e de segurança de TIC para desenvolver sistemas seguros e, também, para construir redes resilientes, capazes de minimizar os riscos e efeitos de um ataque. Ao exigir maiores recursos e tempo dos atacantes, a negação no ciberespaço estabeleceria um modelo de custo-benefício que desestimularia um atacante, sendo assim capaz de eliminar a maioria dos ataques potenciais de atacantes não sofisticados e de atores não estatais. Contudo, ela poderia não ser suficiente para deter Ataques Persistentes Avançados disparados por Estados e inteligências governamentais. Tais ataques são elaborados de forma específica para um determinado alvo, e usam técnicas de invasão contínuas, clandestinas e sofisticadas para obter acesso a um sistema e permanecer dentro dele por um período prolongado, com consequências potencialmente destrutivas. Em geral, são direcionados a alvos de grande valor, como países e grandes corporações, com o objetivo final de roubar informações durante um longo período, ao invés de simplesmente adentrar e sair rapidamente, como muitos *hackers* mal-intencionados fazem durante ataques cibernéticos de nível inferior (Kaspersky, 2018). Já na dissuasão ativa, existiria a ameaça de retaliação ou algum tipo de resposta indesejável que poderia, em nível de beligerância, ir desde negociações diplomáticas até um ataque cinético e uso de força nuclear, passando por sanções econômicas e contra-ataques cibernéticos (Iasiello, 2014).

Para Nye (2016), existem quatro métodos de dissuasão para reduzir e prevenir ações adversas no ciberespaço: punição, negação, emaranhamento[11] e tabus normativos. Em relação à punição, Nye ratifica o que Libicki (2009) afirma sobre esse tipo de dissuasão. No que diz respeito à negação, assevera que, no caso dos Estados Unidos, esse tipo de dissuasão é o que concentra os maiores esforços estratégicos do Pentágono. Em suma, boas defesas cibernéticas podem construir resiliência e boa capacidade de recuperação, e o aumento dos custos pode reduzir o incentivo para alguns ataques potenciais, principalmente, daqueles usuários ou grupos que não são tão sofisticados.

[11] O termo original, em inglês, é *entanglement*.

Ancorado na definição de Snyder (1960), que teoriza que a dissuasão é um conceito mais amplo, e que não precisa contar apenas com a força militar (ou seja, um agressor pode ser inibido pela própria consciência ou, provavelmente, pela perspectiva de perder posição política em relação a outros países), Nye (2016) introduz os mecanismos de dissuasão por emaranhamento e tabus normativos, divergindo da ideia central da adoção da punição e negação como temas centrais para a concepção clássica de dissuasão.

A ideia de dissuasão por emaranhamento se relaciona com a noção da vertente teórica liberal de Relações Internacionais de que a interdependência e o comércio seriam desincentivos ao conflito.[12] O interesse mútuo, portanto, está no cerne desse conceito. Entretanto, expande-se para incluir outros métodos para incentivar a contenção entre os atores, motivando um comportamento responsável dos países através de normas e princípios. Assim, Estados com amplas relações econômicas, diplomáticas e estratégicas, devem calcular até que ponto o comportamento agressivo no ciberespaço poderia afetar potencialmente outros aspectos de suas relações (Nye, 2016).

A noção de dissuasão por tabus normativos foi introduzida por Joseph Nye e acabou, sucessivamente, sendo adotada por outros pesquisadores. Segundo Nye (2016), as normas são como um padrão de comportamento apropriado sobre como uma classe de atores deve agir, ao longo do tempo, quando fornecem ordem, estabilidade e segurança, podendo ser codificadas como leis. Já os tabus são semelhantes às normas, no entanto, têm uma conotação negativa e invertida, pois se referem às formas inapropriadas de agir ou a costumes culturais que estão "fora dos limites".[13] Um exemplo desse tipo de dissuasão foi o acordo, em 2015, entre Estados Unidos e China sobre abster-se de espionagem industrial ou de roubo de propriedade intelectual patrocinada pelo Estado. Isso ocorreu depois que *hackers* chineses roubaram milhões de dados pessoais do *Office of Personnel Management* (OPM), órgão que faz a gestão dos funcionários públicos civis do governo estadunidense. Como resultado, a partir do consenso sino-americano, estabeleceu-se um forte precedente para que outros países, particularmente as grandes e médias potências, não sejam vistos como indo de encontro à convenção estabelecida por um aliado ou adversário mais poderoso.

Cornish (2010), por sua vez, propôs o conceito de dissuasão por associação. Tal conceito é descrito como um mecanismo político

[12] Noção que pode ser encontrada nas ideias de autores e pensadores liberais clássicos - ou "idealistas", como caracterizados pelos pensadores realistas - como Norman Angel (1911) e Woodrow Wilson (1918), mas também de autores de vertentes contemporâneas, como Keohane e Nye (1977), entre outros.

[13] Essas noções se relacionam diretamente com a ideia de interdependência complexa desenvolvida por Nye, em conjunto com Robert Keohane, no livro *Power and interdependence: world politics in transition* (1977). A interdependência complexa procura, entre outros, compreender as condições em que as democracias desenvolvem redes de interdependência e de cooperação e favorecem o surgimento de instituições internacionais que reduzem os riscos de conflitos (Cademartor & Santos, 2016).

para modificar o comportamento de um adversário, seja ele um Estado ou um outro ator, ligando suas atividades predatórias no ciberespaço com sua identidade real. Ao tornar possível identificar e constranger um adversário, exibindo seu comportamento "inapropriado", esse conceito de dissuasão reapresenta a dissuasão por punição, mas agora através de um custo social para os Estados, que pode assumir muitas formas, seja a perda de credibilidade na comunidade internacional, danos à reputação para suas empresas ou ser ostracizado por países de sua comunidade/região.

Em linhas gerais, e no contexto dessa discussão, podemos identificar três desafios principais à dissuasão cibernética. O primeiro é a noção de atribuição, que trata da possibilidade de ter certeza da origem de um ataque. De forma distinta da realidade militar convencional, em que a identificação da origem de eventuais ataques é relativamente fácil, no ambiente cibernético isso se mostra muito mais complexo. Um exemplo claro disso é o caso do Stuxnet, mencionado anteriormente. Se por um lado há diversos indícios que sugerem que o ataque tenha sido lançado por parte das agências de inteligência de Israel e Estados Unidos, como demonstra Kim Zetter (2017), por outro, a comprovação definitiva da autoria é muito difícil. Isso se deve, entre outros, ao fato de que o código usado nesse ataque era auto-replicável, permitindo seu funcionamento independente da atuação de seus desenvolvedores - dificultando, portanto, que se evidencie o vínculo entre ambos. Assim, como destaca Zetter (2017, p. 24), "[...] o ataque era feito essencialmente às cegas. Uma vez lançado, um worm com autopropagação como o Stuxnet cria vida própria, e os atacantes não teriam controle real sobre onde seu código malicioso estaria viajando". Isso, por sua vez, reforça a afirmação feita, em 2010, pelo secretário-adjunto de Defesa dos EUA, William Lynn, de que "[e]nquanto um míssil vem com um endereço de retorno, um vírus de computador geralmente não" (Lynn, 2010, p. 99, tradução nossa).

Isto posto, pode-se dizer que a atribuição é um dos maiores desafios da dissuasão cibernética, especialmente devido à dificuldade forense para identificar um atacante, o que pode demorar meses ou até mesmo não ser possível. Tal dinâmica é significativamente diferente da atribuição nuclear, já que em um contexto em que apenas nove países possuem armamentos de tal natureza, há mais recursos para identificar os materiais necessários para fabricar uma arma, além de existirem diversas barreiras contra aqueles (atores não estatais) que desejam se apropriar de armas e materiais nucleares (Nye, 2016).

No ciberespaço, tal realidade não se reproduz, pois linhas de código-fonte malicioso podem ser desenvolvidas por qualquer pessoa em seu computador, ou até mesmo compradas na *dark web*[14] por atores estatais ou não estatais. Determinar a atribuição no ciberespaço

[14] A *Dark Web* é uma porção da Internet não acessível através de navegadores *web* tradicionais. O acesso requer *softwares*, configurações e autorizações específicas para o acesso. A *Dark Web* é uma pequena porção da chamada *Deep Web*, que é uma parte da rede não indexada pelas ferramentas de busca.

é extremamente difícil, pois os atacantes têm uma infinidade de técnicas de ofuscação para impedir que sejam identificados corretamente ou que identifiquem seu verdadeiro ponto de origem, seja através do comprometimento de uma série de computadores em diferentes países para executar ataques (*botnets*), ou utilizando *proxies*[15] e anonimizadores (Iasiello, 2014).

A atribuição é um componente necessário de qualquer estratégia de dissuasão, pois cabe ao Estado defensor atribuir positivamente um agressor antes do início de qualquer ação retaliatória. No meio militar convencional, também existem dificuldades de atribuição. Em trecho do livro *Fleet Tactics and Coastal Combat* sobre o combate costeiro, Hughes e Girrier (2018) destacam a confusão provocada por comunicações cruzadas nos oceanos. Segundo os autores (Hughes & Girrier, n.p., tradução nossa),

> [a]s águas litorâneas podem ser definidas de forma útil como onde a confusão de comércio costeiro amigo, inimigo e neutro, barcos de pesca, plataformas de petróleo, pequenas ilhas, tráfego aéreo denso, grandes navios comerciais e um intrincado emaranhado de emissões eletrônicas criam um ambiente confuso no qual um ataque furtivo pode ocorrer de repente e quase sem aviso.

No entanto, no contexto do ciberespaço, Healey (2012) construiu uma ferramenta que chamou de "espectro da responsabilidade estatal", que tem como objetivo auxiliar analistas com pouco conhecimento a atribuir responsabilidades por um ataque específico, ou campanha de ataques, com certa precisão e transparência. O espectro tem dez categorias, e cada uma estabelece um grau diferente de responsabilidade, a partir da avaliação da relação de uma nação com um ataque (se ela o ignora, apoia ou conduz). A análise do Estado-nação realizada pela ferramenta produz como resposta um nível de culpabilidade que serve como guia para o tipo e o nível de resposta adequado, que pode ir desde ignorar o ataque até revidar o agressor percebido.

Uma prática de atribuição bem-sucedida no ciberespaço reúne análises técnicas, cognitivas, de inteligência e comportamentais para melhor identificar os atacantes, bem como as influências que podem estar orientando suas operações. A análise técnica não é suficiente para fins de atribuição, pois os atores hostis implementam as mesmas ferramentas, táticas, técnicas e procedimentos. Vários problemas inibem processos de atribuição rápidos e precisos, incluindo o tempo necessário para coletar e analisar o método de ataque empregado e a identificação de motivos, comportamentos e influências externas do ator. No entanto, a fim de evitar constrangimentos públicos e reduzir o volume e a probabilidade de danos colaterais, um nível aceitável de atribuição deve ser realizado antes do início de qualquer ação retaliatória (McKenzie, 2017).

O segundo desafio para a dissuasão cibernética é a comunicação. No livro *Arms and Influence*, Schelling (1966) observa que uma dissuasão bem-sucedida, usando os métodos

[15] Termo utilizado para definir os intermediários entre o usuário e seu servidor.

de punição e negação, dependeria da comunicação efetiva entre um Estado e o ator que desejasse dissuadir. Ou seja, o agente dissuasor deveria ser capaz de comunicar efetivamente à comunidade internacional e, em particular, aos adversários, o que é, ou não, aceitável, e quais seriam as consequências caso esse limite fosse ultrapassado. Assim, um Estado deveria não apenas se pronunciar sobre as atividades que considera que transgridem os limites por ele estabelecidos, mas também estar preparado para agir em resposta a tais ações, sob risco de perder (ou fragilizar) sua credibilidade caso não o fizesse.

Nesse sentido, a comunicação no ciberespaço assume uma função importante, exigindo esforço para se obter consenso para as normas de comportamento nesse ambiente. Tentando identificar uma linguagem comum, em 2013, os Estados Unidos estabeleceram com a China o chamado Diálogo Estratégico e Econômico, para tratar de uma agenda sobre diversos assuntos de economia e segurança, e, inclusive, de questões sobre ataques cibernéticos chineses contra empresas americanas. Nesse campo, entretanto, os diálogos não evoluíram significativamente, sobretudo devido à forma de cada nação abordar o tema. Enquanto os Estados Unidos preferem o termo segurança cibernética para análise dos ativos e ameaças, a China utiliza o termo segurança da informação, que, como visto anteriormente, é mais amplo (Gertz, 2013). Sem um léxico comum entre ambos, as probabilidades de que a comunicação permaneça em desacordo são expressivas, dificultando que se chegue a um consenso, entre eles, sobre como a *Internet* deve ser usada adequadamente.

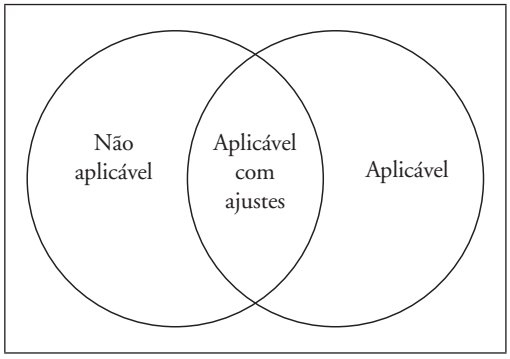
Outra forma de se buscar atingir um acordo sobre normas foi a Convenção Europeia sobre Crimes Cibernéticos de 2001, que fornece um bom quadro de terminologias sobre crimes no ciberespaço. Até o momento, houve sessenta e duas adesões à Convenção. A China não se juntou à Convenção, relatando sua relutância em aceitar uma terminologia acordada pelos Estados ocidentais (Giles; Hagestad, 2013; Council of Europe, 2014).

O terceiro desafio à dissuasão cibernética é a proporcionalidade que, baseando-se nos princípios expressos nas Convenções de Genebra, de 1949, sobre conflito armado, bem como no Manual de Tallinn (Schmitt, 2016), defende a assimilação da guerra cibernética na guerra convencional. Nesse sentido, estabelece-se que uma ação no ciberespaço precisa ser proporcional, principalmente quando essas ações são supostamente provocadas pelos próprios Estados ou por atores patrocinados por eles - ou seja, deve ser comparável e não provocar uma escalada (Jensen, 2012). Por uma série de razões, contudo, é difícil alcançar a proporcionalidade no ciberespaço - isso porque qualquer resposta deve refletir a quantidade (proporcional) do dano causado a um alvo que foi atingido. Portanto, antes da retaliação, que pode ser cinética ou não, um Estado deve avaliar os riscos diplomáticos e econômicos de sua resposta, e todas as suas consequências projetadas, como avaliações de danos de batalha e possíveis efeitos políticos (Iasiello, 2014).

Além dos desafios descritos acima, também devem ser considerados os desafios e possibilidades de aplicação dos sete componentes característicos da dissuasão apresentados anteriormente. A partir de uma análise qualitativa,

tais componentes podem ser classificados em três categorias, no que diz respeito a sua adequação ao ambiente cibernético. A primeira categoria engloba aqueles componentes da dissuasão que poderiam ser aplicados sem restrições ao ambiente cibernético – porquanto, a despeito da existência de características, possibilidades e/ou limitações específicas no ambiente cibernético, estas não seriam suficientes para alterar as características fundamentais do componente ou de seu funcionamento. A segunda categoria, por sua vez, reúne aqueles casos em que as especificidades do ambiente cibernético seriam suficientes para inviabilizar ou esvaziar de sentido um dado componente, que não seria, portanto, aplicável. Por fim, a terceira categoria é composta por aqueles componentes que, ainda que não tenham suas características fundamentais alteradas pelas especificidades da realidade cibernética - sendo, portanto, aplicáveis -, exigem alguma adequação ou ajuste.

Figura 3
Possibilidades de adequação dos componentes da dissuasão convencional ao âmbito cibernético



Fonte: Elaborada pelos autores

Em linhas gerais, os sete componentes inerentes à dissuasão se mostram compatíveis com sua aplicação ao ambiente cibernético, ainda que alguns apresentem desafios. No que diz respeito à apresentação, pelos atores, de um interesse específico a ser protegido, não há qualquer diferença em relação a outras formas de dissuasão - conquanto a tendência seja de que haja uma grande quantidade de interesses simultâneos, dada a existência, no âmbito cibernético, de um número expressivo de ativos que podem, potencialmente, ser alvos de ataques. Nesse sentido, o componente pode ser considerado aplicável, ainda que tal multiplicidade - e simultaneidade - de interesses possa implicar na necessidade de adequações para sua aplicação.

O segundo componente, a declaração dissuasória no âmbito cibernético, por sua vez, consubstancia-se, em linhas gerais, nas estratégias de segurança cibernética dos países, as quais expressam os limites e as possíveis ações retaliatórias em casos de ataque. As estratégias cibernéticas dos países posicionam-se frente aos desafios de segurança de suas infraestruturas críticas, bem como a suas oportunidades de crescimento no âmbito econômico. Em alguns casos, chegam mesmo a apontar seus adversários, como na estratégia estadunidense de 2018, que cita a China e a Rússia como oponentes dos EUA, por exemplo (The White House, 2018). Nesse sentido, apesar de eventuais especificidades, a declaração dissuasória apresenta as mesmas características tanto no âmbito convencional, quanto no cibernético - sendo, portanto, aplicável sem a necessidade de ajustes.

O terceiro componente, as ações de dissuasão, ainda que operem em lógica semelhante a qualquer outra forma de dissuasão, apresentam diferenças no que diz respeito às estratégias punitivas e de negação no âmbito cibernético, devido às dificuldades de identificar os agressores e de dimensionar a proporcionalidade da resposta. Dessa forma, sua aplicação, conquanto possível, apresenta desafios. Para citar a dificuldade de atribuição, Kim Zetter (2017), por exemplo, faz uma comparação entre o desenvolvimento de armas nucleares e armas cibernéticas. Enquanto são grandes as dificuldades - e os custos - para se construir ou obter armas nucleares, o que facilitaria a identificação de eventuais agressores que fizessem uso delas, as armas cibernéticas podem ser facilmente obtidas em mercados paralelos na *Internet*, construídas de forma customizada e até mesmo desenvolvidas por habilidosos programadores destituídos de qualquer qualificação formal, além de poderem ter a origem de sua aplicação "camuflada" pelo uso de ferramentas como *proxies*, tornando a identificação clara e definitiva dos responsáveis por eventuais agressões muito mais complexa. Assim, ainda que em termos abstratos não haja qualquer impedimento à atribuição dos ataques no ambiente cibernético, em termos práticos ela pode se mostrar inalcançável - criando dificuldades, portanto, para as ações de dissuasão.

O quarto componente - a credibilidade -, por sua vez, também é aplicável, mas apresenta peculiaridades relevantes no âmbito cibernético, uma vez que, diferente da dissuasão em outros contextos, a demonstração de capacidades - sistemas e equipamentos - pode mais do que evidenciar a credibilidade das eventuais ameaças - como é o caso, por exemplo, no uso de armamentos convencionais (sejam eles nucleares ou não) - expor as vulnerabilidades do dissuasor. Iniciativas como o *Common Vulnerabilities and Exposures*[16] (CVE) registram, em banco de dados, vulnerabilidades e exposições relacionadas à segurança da informação conhecidas publicamente, o que torna possível a exploração de vulnerabilidades por todo tipo de atacantes: estatais, não-estatais e pessoas comuns. Nesse contexto, se por um lado, tal realidade contribui para que a demonstração de capacidades enquanto estratégia tenha limitações importantes no âmbito cibernético, por outro, todavia, não significa que a credibilidade das eventuais ações de dissuasão expressas na declaração dissuasória sejam inviáveis ou deixem de ter importância - apenas que elas precisam levar tais limitações em consideração.

O quinto componente - a confiança, que trata da punição somente quando o país tiver

[16] O Programa CVE foi lançado em 1999 e é uma iniciativa colaborativa de diversas organizações de tecnologia e segurança. Sua missão é identificar, definir e catalogar vulnerabilidades de segurança cibernética divulgadas publicamente. Existe um registro CVE para cada vulnerabilidade no catálogo. As vulnerabilidades são descobertas, atribuídas e publicadas por organizações de todo o mundo que têm parceria com o Programa CVE. Os parceiros publicam registros CVE para comunicar descrições consistentes de vulnerabilidades. Profissionais de tecnologia da informação e cibersegurança usam registros CVE para garantir que estão discutindo o mesmo problema e para coordenar seus esforços para priorizar e resolver as vulnerabilidades.

seus interesses violados -, também se expressa de forma distinta no âmbito do ciberespaço, já que os ataques são furtivos e podem ser disparados, em princípio com a mesma facilidade, por atores estatais ou não-estatais, o que pode contribuir para que uma agressão possa levar a uma escalada de ataques cibernéticos como resposta. Mostra-se relevante, nesse contexto, a consideração apresentada por Zettel (2017) a respeito do ataque cibernético promovido pelos EUA e por Israel contra o Irã. Como destaca a autora, tal ação teria aberto um importante precedente, porquanto teria sido realizada com o objetivo de atender a interesses políticos e de segurança nacional dos dois agressores, sem que existisse um contexto de guerra declarada entre eles e o Irã - o que poderia ter funcionado não como uma ação de dissuasão, mas sim como um incentivo para que esse país promovesse ataques em resposta (Zettel, 2017). Assim sendo, ainda que a natureza do ambiente cibernético e suas especificidades - sobretudo a dificuldade de atribuição de eventuais ataques - criem contextos em que a preocupação com a confiança pareça poder ser dispensada pelos atores, ela se mantém fundamental para distinguir um cenário de dissuasão - no qual se evita que um ataque seja sofrido sem a necessidade de que seja realizado um ataque a outro ator - de um de agressão direta.

Em relação ao medo, percebe-se que, no contexto do ciberespaço, ele se caracteriza não necessariamente pelo receio de uma eventual retaliação militar, mas geralmente pelo temor de consequências com um maior custo social, atingindo os países em seus laços comerciais e diplomáticos e, consequentemente, impactando também os atores não-estatais. Nesse sentido, enquanto os Estados costumam recorrer à diplomacia como forma de evitar os custos - não apenas econômicos, mas também políticos, sociais, humanos, etc. - dos conflitos convencionais, nucleares ou não (o que ficou claro, por exemplo, na chamada Crise dos Mísseis, em 1962, entre EUA e URSS), tal realidade pode se mostrar bastante distinta no ambiente cibernético. Isso se dá, entre outros motivos, porque diante da possibilidade da realização de ataques anônimos, os quais tendem a diminuir significativamente - ou até mesmo eliminar - eventuais custos e/ou consequências deles decorrentes (e, portanto, o medo), podem se reduzir os incentivos à negociação e à diplomacia, incrementando os incentivos à realização de ataques (Zettel, 2017). Destarte, ainda que o medo enquanto componente da dissuasão tenha importância também no ambiente cibernético, sua consideração, nesse contexto, certamente apresenta limitações significativas.

Por fim, o sétimo componente, o cálculo de custo-benefício, que está na essência da eficácia da dissuasão, é realizado por todos os atores (sejam eles estatais ou não) na consideração da viabilidade (e dos potenciais ganhos auferidos com) de eventuais ataques. Mesmo que tal componente tenha especificidades particulares ao ambiente cibernético - por exemplo o fato de que, pela sua forma de concepção, as armas cibernéticas deixam rastros de sua construção no código-fonte, permitindo que o ator agredido, caso consiga decifrar o código, aproprie-se dele e até mesmo o aprimore, incrementando, assim, seu próprio "arsenal" (Zettel, 2017) - a decisão de realizar, ou não, um ataque

sempre levará em conta o cálculo da relação custo-benefício de tal ação, sendo, portanto, o componente plenamente aplicável também ao âmbito cibernético. O quadro 1, abaixo, busca sintetizar a adequação desses componentes à noção de dissuasão cibernética, bem como os eventuais desafios a sua aplicação.

Quadro 1
Aplicações e desafios dos componentes da dissuasão convencional na dissuasão cibernética

COMPONENTE	ADEQUAÇÃO	SEMELHANÇAS	LIMITAÇÕES
Interesse	Aplicável com ajustes	Apresentação, por parte dos Estados, de suas prioridades de proteção dos ativos críticos.	Existência de um número muito grande de vetores de possíveis ataques, que podem ser ativos de tecnologia e seres humanos, ambos necessitando de estratégias de proteção que vão desde a aplicação de ferramentas de *software* de proteção às estratégias de educação e conscientização.
Declaração dissuasória	Aplicável	Presentes nas estratégias de segurança e defesa cibernéticas dos países, nas quais estes expressam os limites e ações retaliatórias em casos de ataque.	-
Ações de dissuasão	Aplicável com ajustes	Possibilidade de apresentar ameaças de retaliação e imposição de custos a potenciais agressores e/ou demovê-los de sua intenção por meio da redução dos eventuais benefícios resultantes da ação.	Atribuir a origem real do ataque ainda é um desafio para a segurança cibernética. Além disso, existe a dificuldade de saber dosar a força para uma resposta em caso de ataque cibernético. Ações de punição são mais diretamente atingidas pelas limitações do que as de negação.
Credibilidade	Aplicável com ajustes	As ações de dissuasão precisam ser comunicadas à comunidade internacional, particularmente aos adversários, sobre os limites aceitáveis.	Maior facilidade para realização de ataques sem atribuição, aumentando os incentivos para a realização de ataques de natureza não-retaliatória. Inexistência de um fórum centralizado para a normatização de crimes e seus respectivos limites. Alguns países preferem adotar suas próprias normas sobre crimes cibernéticos, o que dificulta o entendimento, principalmente nos casos que envolvem a espionagem cibernética.

Confiança	Aplicável com ajustes	Entendimento da necessidade (e possibilidade) de garantia de que não haverá punições caso não haja ataques contra o interesse que está sendo protegido.	No ambiente cibernético, os ataques são furtivos e podem ser disparados, sem grandes distinções, por atores estatais e não-estatais, o que pode levar a uma escalada de ataques cibernéticos como resposta, colocando em dúvida a garantia de que não haverá punições se um interesse/ativo não for desrespeitado no ciberespaço.
Medo	Aplicável com ajustes	Os Estados, devido aos potenciais custos materiais e também sociais, estão suscetíveis ao medo.	Outros atores, que não os Estados, podem ter menos "medo"/receio, uma vez que podem ser menos suscetíveis aos potenciais custos de eventuais ataques.
Custo-benefício	Aplicável	O interesse mútuo e a interdependência no comércio são importantes para países com múltiplos laços comerciais e políticos, podendo não afetar aqueles com poucos laços no cenário internacional.	-

Fonte: Elaborado pelos autores.

5. CONSIDERAÇÕES FINAIS

O ambiente cibernético apresenta, inegavelmente, muitas características próprias, que o distinguem - seja no âmbito securitário ou não - do "mundo concreto" (não-cibernético). A análise aqui proposta, contudo, demonstra que apesar dessas diferenças, o conceito de dissuasão - tradicionalmente aplicado às ameaças militares no âmbito não-cibernético - pode, sim, ser aplicado ao ambiente cibernético, ainda que grande parte de seus componentes apresente algum desafio em sua operacionalização. Nesse sentido, ainda que o conceito de "dissuasão cibernética" encontre similaridade com a teoria de dissuasão convencional, sendo composto por elementos como punição, negação, atribuição e comunicação - os quais estruturam o modelo convencional -, a natureza e as características do ambiente cibernético exigem que sejam feitas adaptações para garantir sua aplicabilidade.

Diante do exposto neste artigo, pode-se dizer que grande parte das dúvidas em relação à aplicação do conceito de dissuasão ao ambiente cibernético é criada pela dificuldade de atribuir, com clareza, a origem de qualquer ataque realizado no ambiente cibernético, o que se deve essencialmente à natureza do ciberespaço. Ainda que as limitações existentes no que diz respeito à comunicação e à proporcionalidade sejam relevantes, ambos elementos também são permeados pelas próprias limitações pertinentes à questão da atribuição. Tal contexto também se expressa em relação aos componentes característicos da dissuasão convencional aqui

identificados – interesse, declaração dissuasória, ações de dissuasão, credibilidade, confiança, medo e cálculo custo-benefício.

Dos sete componentes, apenas dois - a adoção de uma declaração dissuasória por parte do agente dissuasor e a realização de um cálculo de custo-benefício por parte do potencial agressor - têm as mesmas características (e limitações) e respondem às mesmas lógicas em ambos os cenários, convencional e cibernético. Nesse sentido, apesar de apresentar características e dinâmicas próprias, a realidade cibernética não apresenta qualquer desafio à aplicação desses conceitos. No caso dos demais componentes, todavia, a realidade que se apresenta é distinta. Conquanto a lógica por trás de cada um deles seja a mesma tanto no âmbito convencional, quanto no cibernético, as especificidades do mundo cibernético criam novas possibilidades e/ou limitações que impõem desafios à aplicação de tais conceitos.

Conforme mencionado, a dificuldade de atribuição é, certamente, a característica mais relevante do ambiente cibernético nesse contexto, uma vez que grande parte dos desafios impostos à aplicação dos componentes da dissuasão convencional ao ambiente cibernético são consequência dela. A possibilidade de realização de ataques cuja origem seja difícil de identificar seguramente não impossibilita sua dissuasão, conquanto possa criar incentivos para sua execução. Ainda assim, contudo, as potenciais consequências da eventual identificação da origem desses ataques - ou mesmo de retaliações sem que haja a devida atribuição -, que podem redundar inclusive em respostas cinéticas a eventos cibernéticos, parecem se consubstanciar em elementos importantes não apenas no que diz respeito à componente do medo, mas também no caso do cálculo custo-benefício, contribuindo, por sua vez, para, em oposição à dificuldade de atribuição, diminuir os incentivos aos ataques. De forma semelhante, o fato de que a realização de ataques cibernéticos pode redundar não apenas em transferência de tecnologia do atacante ao atacado, mas também na exposição de suas vulnerabilidades, também contribui para desincentivar eventuais ataques, uma vez que seus potenciais custos acabam sendo significativamente elevados. Nesse sentido, se por um lado as características do mundo cibernético podem criar incentivos aos ataques - a ponto de diminuir a relevância e/ou pertinência do conceito de dissuasão -, por outro, podem diminuir tais incentivos - ou mesmo criar desincentivos -, reforçando a importância e/ou possibilidade de aplicação do conceito.

Cumpre ressaltar, por fim, que mesmo com as inúmeras consequências impostas pela natureza do ambiente cibernético e suas especificidades, nenhuma de suas características parece se mostrar suficiente para tornar algum dos componentes da dissuasão convencional irrelevante ou não-aplicável. Isto posto, parece-nos que, a despeito de apresentar limitações, desafios e particularidades em relação ao modelo convencional, o conceito de dissuasão apresenta a mesma relevância e aplicabilidade tanto no âmbito convencional, quanto no cibernético.

REFERÊNCIAS

ABNT. (2015). *ABNT NBR ISO/IEC 27032. Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética*. Brasília: Associação Brasileira de Normas Técnicas.

Allison, G. T. (1971). *Essence of decision: explaining the Cuban missile crisis*. Boston: Little, Brown.

Angell, N. (1911). *The great illusion: a study of the relation of military power in nations to their economic and social advantages*. Toronto: Mcclelland and Goodchild.

Australian Government. (2020). *Australia's Cyber Security Strategy* 2020. Australian Government Department of Home Affairs. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Brantly, A. (2018). The Cyber Deterrence Problem. In T. Minárik, R. Jakschis, & L. Lindström (Eds.), *2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects* (pp. 31–54). Tallinn: Nato Cooperative Cyber Defence Centre of Excellence.

Brasil. (2014). *MD31-M-07 Doutrina Militar de Defesa Cibernética*. Obtido do Ministério da Defesa website: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf

Brasil. (24/07/2020). Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Obtido em 2 de novembro de 2020, do: http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica

Brodie, B. (1959). *Strategy in the Missile Age*. Santa Monica: Rand.

Brodie, B. (Ed.). (1946). *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Co.

Cademartor, L. H. U., & Santos, P. C. (2016). A Interdependência Complexa e a Questão dos Direitos Humanos no Contexto das Relações Internacionais. *Revista Brasileira de Direito*, *12*(2), 71–81. https://doi.org/10.18256/2238-0604/revistadedireito.v12n2p71-81

Clarke, R. A., & Knake, R. (2011). *Cyber War*. New York: Harpercollins.

Cornish, P. (2010). Arms control tomorrow: the challenge of nuclear weapons in the twenty-first century. In: R. Niblett (Ed.). *America and a Changed World: A Question of Leadership*, (pp.223–237).

Council of Europe. (2014). Convention on Cybercrime. Obtido em 31 de outubro de 2020, do website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

Dhillon, G. (2007). *Principles of information systems security: text and cases*. Hoboken, Nj: Wiley, C.

Doffman, Z. (06/05/2019). Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First. Obtido em 2 de novembro de 2020, do website: https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/?sh=6a5bfcc7afb5

Ferraço, R. (2014). *CPI Da Espionagem Relatório Final*. Obtido do website: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco

Geers, K. (2011). *Strategic Cyber Security*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

George, A. L., & Smoke, R. (1974). *Deterrence in American foreign policy: theory and practice*. New York: Columbia University Press.

Gertz, B. (/16/07/2013). U.S., China Conclude Strategic and Economic Dialogue Talks. Obtido em 31 de outubro de 2020 do Washington Free Beacon website: https://freebeacon.com/national-security/u-s-china-conclude-strategic-and-economic-dialogue-talks/

Giles, K., & Hagestad, W. (2013, June 1). Divided by a common language: Cyber definitions in Chinese, Russian and English. Obtido em 4 de novembro de 2020 do IEEE Xplore website: https://ieeexplore.ieee.org/abstract/document/6568390

Gobierno de España. (2019). *Estrategia Nacional de Ciberseguridad 2019*. Departamento de seguridad nacional. https://www.dsn.gob.es/ca/file/2989/download?token=EuVy2lNr#:~:text=Spain

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly*, *4*(3), 102–135.

Gray, C. S. (1990). The definitions and assumptions of deterrence: Questions of theory and practice. *Journal of Strategic Studies*, *13*(4), 1–18. https://doi.org/10.1080/01402399008437428

Gray, C. S. (1999). *The second nuclear age*. Boulder: Lynne Rienner.

Healey, J. (22/02/2012). Beyond Attribution: Seeking National Responsibility in Cyberspace. Obtido em 30 de outubro de 2020 do Atlantic Council website: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/

Hughes, W. P., & Girrier, R. (2018). *Fleet tactics and naval operations* (2ª ed.). Annapolis, Maryland: Naval Institute Press.

Iasiello, E. (2014). Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*, *7*(1), 54–67. https://doi.org/10.5038/1944-0472.7.1.5

IDF, I. D. F. (05/05/2019). *Cleared for Release*. Obtido em 17 de outubro de 2020 do Twitter: https://twitter.com/IDF/status/1125066395010699264?s=20

ISO, I. O. for S. (2018). *ISO/IEC 27000. Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*. ISO - International Organization for Standardization.

Janis, I. L. (1982). *Groupthink: psychological studies of policy decisions and fiascoes*. Boston: Houghton Mifflin.

Jensen, E. (2012). Cyber Deterrence. *Emory International Law Review*, *26*(2), 773–824. https://digitalcommons.law.byu.edu/faculty_scholarship/231/

Jervis, R. (1979). Deterrence Theory Revisited. *World Politics*, *31*(2), 289–324. https://doi.org/10.2307/2009945

Jervis, R., Lebow, R. N., & Stein, J. G. (1985). *Psychology and deterrence*. Baltimore: Johns Hopkins University Press.

Karpavičiūtė, I. (2019). Strategic Stability: It Takes Two to Tango? *Lithuanian Annual Strategic Review*, *17*(1), 97–121. https://doi.org/10.2478/lasr-2019-0004

Kaspersky. (08/11/2018). O que é uma ameaça persistente avançada (APT)? Obtido em 1º de novembro de 2020, do: www.kaspersky.com.br website: https://www.kaspersky.com.br/resource-center/definitions/advanced-persistent-threats

Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence: world politics in transition*. Boston: Little, Brown.

Klimburg, A. (Ed.). (2012). *National cyber security framework manual*. Tallinn: Nato Cooperative Cyber Defense Centre of Excellence.

Knopf, J. W. (2010). The Fourth Wave in Deterrence Research. *Contemporary Security Policy*, *31*(1), 1–33. https://doi.org/10.1080/13523261003640819

Lewis, J. A. (2009) *Fog of Cyberwar: Discouraging Deterrence*. Switzerland: International Relations and Security Network.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, Ca: Rand.

Long, A. G. (2008). *Deterrence-From Cold War to long war: lessons from six decades of RAND research*. Santa Monica: RAND.

Lupovici, A. (2010). The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda. *International Studies Quarterly*, *54*(3), 705–732. https://doi.org/10.1111/j.1468-2478.2010.00606.x

Lynn, W. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, *89*(5), 97–108. https://www.jstor.org/stable/20788647

McKenzie, T. M. (2017). *Is cyber deterrence possible?* Alabama: Air University Press, Air Force Research Institute.

Mearsheimer, J. J. (1981). *The theory and practice of conventional deterrence* (PhD Thesis.; p. 485). Cornell University.

Morgan, P. M. (2003). *Deterrence now*. Cambridge: Cambridge University Press.

Muller, R. (2004). The Origins of MAD: A Short History of City-Busting. In H. D. Sokolski (Ed.), *Getting MAD Nuclear mutual assured destruction, its origins and practice* (pp. 15–50). Carlisle: Strategic Studies Institute.

Myers, J., & Whiting, K. (2019, January 16). These are the biggest risks facing our world in 2019. Obtido em 27 de outubro de 2020 do World Economic Forum website: https://www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019/

Newman, L. H. (2019, May 6). What Israel's Strike on Hamas Hackers Means For Cyberwar. *Wired*. Retrieved from https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

Nye, J. (2016). Deterrence and Dissuasion in Cyberspace. *Journal of Cyber Policy*, *1*(2), 44–71. https://doi.org/10.1162/ISEC_a_00266

Putten, F.-P. V. D., Meijnders, M., & Rood, J. (2015). *Deterrence as a security concept against non-traditional threats* (pp. 1–64). Obtido do website: https://www.clingendael.org/sites/default/files/pdfs/deterrence_as_a_security_concept_against_non_traditional_threats.pdf

República de Colombia. (2016). *Política Nacional de Seguridad Digital*. Consejo Nacional de Política Económica y Social: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y

Ryan, N. J. (2017). Five Kinds of Cyber Deterrence. *Philosophy & Technology*, *31*(3), 331–338. https://doi.org/10.1007/s13347-016-0251-1

Samson, V., & Weeden, B. (Eds.). (2020). Global Counterspace Capabilities: An Open Source Assessment. Obtido do Secure World Foundation website: https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf

Schelling, T. C. (1960). *The strategy of conflict*. Cambridge: Harvard University Press.

Schelling, T. C. (1966). *Arms and Influence*. New Heaven: Yale University Press

Sêmola, M. (2014). *Gestão da Segurança da Informação: uma visão executiva* (2ª ed.). Rio de Janeiro: Elsevier.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know*. Oxford: Oxford University Press.

Snyder, G. (1961). *Deterrence or Defense*. Princeton: Princeton University Press.

Snyder, G. H. (1960). Deterrence and power. *Journal of Conflict Resolution*, *4*(2), 163–178. https://doi.org/10.1177/002200276000400201

Steinbruner, J. (1976). Beyond Rational Deterrence: The Struggle for New Conceptions.

World Politics, *28*(2), 223–245. https://doi.org/10.2307/2009891

Syeed, N. (12/04/2017). Outer-Space Hacking a Top Concern for NASA's Cybersecurity Chief. *Bloomberg.com*. Obtido do website: https://www.bloomberg.com/news/articles/2017-04-12/outer-space-hacking-a-top-concern-for-nasa-s-cybersecurity-chief

Ten, C.-W., Manimaran, G., & Liu, C.-C. (2010). Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *40*(4), 853–865. https://doi.org/10.1109/tsmca.2010.2048028

The White House. (2011). International Strategy for Cyberspace. Obtido do White House website: https://assets.documentcloud.org/documents/2700127/Document-46.pdf

The White House. (2018). *National Cyber Strategy of the United States of America*. Obtido do Trump White House Archives: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Thucydides. (2009). *The Peloponnesian War* (M. Hammond, Trans.). Oxford: Oxford University Press.

Ventures, C. (2020). *2019 Official Annual Cybercrime Report*. Obtido website: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Villa, R. A. D. (2006). A segurança internacional no pós-guerra fria: um balanço da teoria tradicional e das novas agendas de pesquisa. *Bib: Revista Brasileira de Informação Bibliográfica Em Ciências Sociais*, *62*(2° semestre), p. 19-31.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*(1), 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Walt, S. M. (1991). The Renaissance of Security Studies. *International Studies Quarterly*, *35*(2), 211–239. https://doi.org/10.2307/2600471

Wilner, A. (2017). Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy*, *36*(4), 309–318. https://doi.org/10.1080/01495933.2017.1361202

Wilson, W. (1918). *President Woodrow Wilson's Fourteen Points*. Obtido do website: https://avalon.law.yale.edu/20th_century/wilson14.asp

Wohlstetter, A. (1959). The Delicate Balance of Terror. *Foreign Affairs*, *37*(2), 211–234. https://doi.org/10.2307/20029345

Wolfers, A. (1946). The Atomic Bomb and Soviet-American relation. In B. Brodie (Ed.), *The Absolute Weapon: Atomic Power and World Order* (pp. 90–123). New York: Harcourt, Brace and Co.

Zetter, K. (2017). *Contagem Regressiva Até Zero Day*. Rio de Janeiro: Brasport.