ISBN: 978-65-986235-3-1

Aurum EDITORA

CAPÍTULO 16

CIBERSEGURANÇA E CONFLITOS GLOBAIS: UMA ANÁLISE QUALITATIVA DAS RELAÇÕES INTERNACIONAIS NA ERA DIGITAL

CYBERSECURITY AND GLOBAL CONFLICTS: A QUALITATIVE ANALYSIS OF INTERNATIONAL RELATIONS IN THE DIGITAL AGE

https://doi.org/10.63330/aurumpub.005-016

Marcelo da Silva Lima
Segurança Cibernética

RESUMO

A segurança cibernética é o tema central deste trabalho, que analisa seus principais desafios e oportunidades no contexto global contemporâneo. O estudo parte da constatação de que, com o avanço acelerado das tecnologias da informação e comunicação, o ciberespaço tornou-se um domínio estratégico para Estados, empresas e cidadãos, exigindo respostas institucionais cada vez mais sofisticadas frente ao crescimento das ameaças digitais. O objetivo principal da pesquisa é examinar criticamente os riscos relacionados à cibersegurança e identificar as potencialidades que esse campo oferece nas esferas política, econômica e social. A metodologia utilizada foi qualitativa, com base em revisão bibliográfica e documental de autores e instituições de referência, como Singer e Friedman, Nocetti, Nye, Clarke e Knake, OCDE, Fórum Econômico Mundial, entre outros. O trabalho estrutura-se em três capítulos. O primeiro apresenta a evolução do conceito de segurança cibernética e sua inserção na agenda internacional, destacando a crescente relevância do tema no desenvolvimento econômico e na governança global. O segundo capítulo aborda os principais desafios, com ênfase no problema da atribuição de ataques, nas vulnerabilidades das infraestruturas críticas e no risco de escalada de tensões geopolíticas. Também são discutidos fenômenos como botnets, hacktivismo e o "paradoxo da conectividade", que torna os países mais avançados tecnologicamente os mais expostos a ameaças. No terceiro capítulo, são analisadas as oportunidades da segurança cibernética, com destaque para o fortalecimento da economia digital, a criação de empregos especializados, a cooperação internacional e o estímulo à educação e à inclusão digital. Entre os resultados obtidos, conclui-se que a segurança cibernética, além de um desafio técnico e geopolítico, é também uma oportunidade estratégica de inovação, integração institucional e fortalecimento da cidadania digital. A pesquisa evidencia que uma abordagem colaborativa, baseada em planejamento, resiliência e governança participativa, é essencial para transformar o ambiente digital em um espaço mais seguro, confiável e inclusivo.

Palavras-chave: Segurança cibernética; Tecnologia da informação; Ambiente digital.

ABSTRACT

Cyber security is the central theme of this work, which analyzes its main challenges and opportunities in the contemporary global context. The study starts from the realization that, with the accelerated advance of information and communication technologies, cyberspace has become a strategic domain for states, companies and citizens, requiring increasingly sophisticated institutional responses to the growth of digital threats. The main objective of the research is to critically examine the risks related to cybersecurity and identify the potential that this field offers in the political, economic and social spheres. The methodology used was qualitative, based on a bibliographical and documentary review of leading authors and institutions, such as Singer and Friedman, Nocetti, Nye, Clarke and Knake, the OECD and the World Economic Forum, among others. The work is structured in three chapters. The first presents the evolution of the concept of cyber security and its inclusion on the international agenda, highlighting the growing relevance of the issue

in economic development and global governance. The second chapter addresses the main challenges, with an emphasis on the problem of attributing attacks, the vulnerabilities of critical infrastructures and the risk of escalating geopolitical tensions. Phenomena such as botnets, hacktivism and the “connectivity paradox”, which makes the most technologically advanced countries the most exposed to threats, are also discussed. In the third chapter, the opportunities of cyber security are analyzed, with emphasis on strengthening the digital economy, creating specialized jobs, international cooperation and stimulating education and digital inclusion. Among the results obtained, it is concluded that cyber security, in addition to being a technical and geopolitical challenge, is also a strategic opportunity for innovation, institutional integration and strengthening digital citizenship. The research shows that a collaborative approach, based on planning, resilience and participatory governance, is essential for transforming the digital environment into a safer, more reliable and inclusive space.

Keywords: Cyber security; Information technology; Digital environment.

1 INTRODUÇÃO

A presente pesquisa tem como tema central a segurança cibernética, cuja relevância tem crescido de forma exponencial na agenda internacional, acompanhando o avanço das tecnologias da informação e da comunicação. Com o surgimento de novas ameaças digitais, a segurança no ciberespaço tornou-se uma das principais preocupações de Estados, empresas e cidadãos, exigindo análises aprofundadas sobre seus desafios e oportunidades.

Segundo Nye (1998), a globalização pode ser compreendida como um processo decorrente do crescimento e da atuação de novos atores no cenário internacional — como organizações internacionais, empresas multinacionais, organizações não governamentais e outras entidades — que investem em mecanismos de expansão e influência no Sistema Internacional. Essa dinâmica favorece a cooperação entre atores estatais e não estatais, contribuindo para relações mais pacíficas e funcionais, com impacto positivo sobre o desenvolvimento e a manutenção da paz. Já sob a perspectiva de Lévy (1999), a globalização é impulsionada pelo progresso tecnológico internalizado pela sociedade. Para ele, essa transformação social avança com maior rapidez do que a capacidade dos Estados de desenvolver ferramentas adequadas, criando um novo ambiente informacional que reduz distâncias e inaugura novas realidades, como a internet.

Buzan (1998), por sua vez, interpreta a globalização como uma consequência dos investimentos estatais em novas formas de poder, o que fomenta o desenvolvimento de tecnologias que alimentam disputas no Sistema Internacional — sejam elas econômicas, militares ou tecnológicas. Em comum, todas essas visões destacam a relação intrínseca entre globalização e o avanço tecnológico, sugerindo que a segurança cibernética se insere nesse contexto como um elemento estratégico decorrente da crescente interconectividade e interdependência global, com repercussões amplas nos campos social, econômico, político e cultural.O estudo está fundamentado em uma revisão bibliográfica que inclui autores como Singer e Friedman (2014), Nocetti (2018), Nye (2010), Clarke e Knake (2015), entre outros, que oferecem contribuições fundamentais para o entendimento da complexidade do tema. O objetivo geral deste trabalho é analisar criticamente os principais desafios enfrentados pelos Estados e pelas instituições no âmbito da segurança cibernética, ao mesmo tempo em que se investigam as oportunidades que esse campo oferece nas esferas política, econômica e social. Parte-se da hipótese de que, apesar dos riscos associados à crescente digitalização, a segurança cibernética também pode se configurar como vetor de desenvolvimento estratégico, inovação tecnológica e cooperação internacional. Justifica-se esta pesquisa pela necessidade urgente de compreender o impacto das ameaças digitais na estabilidade das democracias, na integridade das infraestruturas críticas e na confiança dos usuários nas tecnologias digitais, além de propor caminhos que visem à construção de uma governança mais eficaz no ciberespaço.

A metodologia adotada é qualitativa, com base em pesquisa bibliográfica e documental. O trabalho

encontra-se estruturado em três capítulos principais. O primeiro capítulo trata da segurança cibernética no cenário internacional, abordando sua emergência como tema de segurança global, com destaque para o papel da internet e das TICs no desenvolvimento econômico e social e a crescente sofisticação das ameaças cibernéticas, conforme demonstrado em relatórios da OCDE (2012) e do Fórum Econômico Mundial (2018).

O segundo capítulo, intitulado Novos desafios, discute o problema da atribuição de ataques cibernéticos, as vulnerabilidades das infraestruturas críticas e os riscos de escalada de tensões entre Estados. São abordados conceitos como *botnets*, *hacktivismo*, espionagem digital e o "paradoxo da conectividade", que evidencia como os países mais tecnologicamente avançados são também os mais vulneráveis, conforme destacam Gartzke (2013) e o relatório *Strategic Survey 2018* (IISS, 2018).

O terceiro capítulo explora as oportunidades relacionadas à segurança cibernética, especialmente nas áreas da economia, das relações internacionais e da cidadania digital. Discute-se como a cibersegurança pode fomentar a criação de empregos, promover o desenvolvimento de novos setores de tecnologia e fortalecer a cooperação entre países na formulação de normas e políticas internacionais para a proteção do ciberespaço.

Por fim, o trabalho é concluído com uma reflexão sobre a importância de uma abordagem integrada e colaborativa para enfrentar os desafios da segurança cibernética e aproveitar suas oportunidades, reforçando a necessidade de investimentos contínuos em tecnologia, educação digital, governança e resiliência institucional. O estudo pretende, assim, contribuir para o debate acadêmico e prático sobre a construção de um ambiente digital mais seguro, inclusivo e confiável.

2 DESENVOLVIMENTO

2.1 SEGURANÇA CIBERNÉTICA

Até o final do século XX, a agenda de segurança internacional era tradicionalmente dominada por certos temas, como os conflitos entre e dentro dos Estados, além da segurança ambiental e da segurança humana. Contudo, com a virada do milênio e o início do século XXI, surge um novo tópico de destaque: a cibersegurança (cybersecurity). Esse novo eixo de preocupação está diretamente relacionado à revolução tecnológica e informacional vivenciada desde os anos finais do século passado, marcada, sobretudo, pela rápida disseminação de informações e pela redução contínua de seus custos. Devido à constante evolução tecnológica associada ao tema, a cibersegurança demanda atualização frequente, visto que suas ferramentas e métodos estão em constante aperfeiçoamento.

Em 2012, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou o relatório *Cybersecurity Policy Making at a Turning Point*, no qual avaliou as estratégias de cibersegurança de dez países membros. O documento (OCDE, 2012) evidenciou dois aspectos recorrentes nessas políticas

nacionais: (i) o papel central da internet e das tecnologias da informação para o crescimento econômico e social, sendo tratadas como infraestrutura essencial; e (ii) o crescimento veloz e constante das ameaças cibernéticas.

Esse entendimento foi reforçado por Jean-Yves Le Drian, então ministro das Relações Exteriores da França, durante a 72ª Assembleia Geral da ONU, em setembro de 2017. Para ele, o ciberespaço se consolidou como um novo ambiente de oportunidades econômicas e transformações sociais. No entanto, ele alertou para as vulnerabilidades emergentes do ambiente digital, que podem ameaçar os princípios fundamentais de abertura e liberdade que sustentam o ciberespaço, além de comprometer as vantagens econômicas da revolução digital. Le Drian advertiu que as ameaças estão se multiplicando nesse ambiente, configurando um desafio central, ainda em seus estágios iniciais, e que tende a se agravar nos próximos anos.

Jean-Claude Juncker, então presidente da Comissão Europeia, também enfatizou a gravidade das ameaças digitais ao afirmar, em seu discurso sobre o estado da União, em 2017, que "os ataques cibernéticos podem ser mais perigosos para a estabilidade das democracias e das economias do que armas e tanques".

Nye (2018) corrobora essa visão ao observar que, desde 2013, o Diretor de Inteligência Nacional dos Estados Unidos passou a considerar os riscos cibernéticos como a maior ameaça à segurança nacional. De forma semelhante, o relatório *Strategic Survey 2018: The Annual Assessment of Geopolitics*, do International Institute for Strategic Studies (IISS), salienta que a revolução digital está impactando profundamente todos os elementos da arte de governar (statecraft), como a diplomacia, os serviços de inteligência e o uso da força.

No campo econômico, especialmente no setor financeiro, Boer e Vazquez (2017) apontam dados alarmantes sobre os prejuízos causados por ciberataques. Um estudo do Lloyd's of London, realizado em julho de 2017, indicava que um ataque cibernético global poderia gerar perdas superiores a 121 bilhões de dólares. Já o *Global Risks Report 2018*, do Fórum Econômico Mundial, baseado em pesquisa do Juniper Research, estimou que o custo global do cibercrime para as empresas entre 2017 e 2022 chegaria a 8 trilhões de dólares.

Dessa forma, a relevância da cibersegurança no cenário internacional contemporâneo aumenta de forma acelerada. Por isso, investigar a segurança no ciberespaço tornou-se essencial para a formulação de políticas e a tomada de decisões por parte dos atores das relações internacionais. Assim, compreender o que configura o ciberespaço representa um ponto inicial fundamental para tais análises.

2.2 NOVOS DESAFIOS

Um dos principais obstáculos enfrentados no campo da segurança cibernética é o problema da atribuição, ou seja, a dificuldade em identificar de forma precisa o autor de um ataque digital. Essa limitação

compromete a capacidade de resposta dos Estados, uma vez que impossibilita medidas de retaliação claras e eficazes, inviabilizando o pleno exercício do direito à legítima defesa (SINGER; FRIEDMAN, 2014; NOCETTI, 2018). Conforme destacam Singer e Friedman (2014), os atacantes frequentemente recorrem a malwares — softwares maliciosos — que permitem controlar, sem o conhecimento do usuário, dispositivos pessoais conectados à internet. Esses computadores passam a compor redes chamadas botnets, usadas com frequência em ataques de negação de serviço (DDoS), dificultando ainda mais a identificação da origem dos ataques.

Três características dessas botnets são ressaltadas por Singer e Friedman (2014): a ausência de fronteiras geográficas, a ignorância do proprietário em relação à utilização indevida de sua máquina e, por fim, a limitação da investigação técnica, que geralmente consegue rastrear apenas até o dispositivo intermediário utilizado, e não ao verdadeiro autor do ataque. Assim, a atribuição formal de ataques cibernéticos torna-se incomum, sendo frequentemente motivada mais por razões políticas do que por provas técnicas incontestáveis (NOCETTI, 2018). Gartzke (2013, p. 46) reforça esse ponto ao afirmar que "os atacantes têm maior propensão a agir quando sabem que é improvável sofrerem retaliação".

Esse contexto leva à utilização de estratégias de disfarce, como a negação de envolvimento estatal e a atribuição dos ataques a grupos civis ou ativistas digitais, os chamados "cibercidadãos" ou *netizens* (FERNANDES, 2012). Uma forma de ação comum nesses casos é o hacktivismo, definido por Singer e Friedman (2014, p. 77) como o uso de meios cibernéticos não violentos — ainda que legalmente questionáveis — para promover ou resistir a mudanças sociais ou políticas. Os hacktivistas podem atuar individualmente ou em coletivos descentralizados, como o Anonymous, ou ainda em organizações mais estruturadas. Um exemplo notável é o uso de grupos terceirizados suspeitos de desenvolver armas cibernéticas em nome do governo russo, tornando incerta a origem real dos ataques — como ocorreu durante a "guerra cibernética da Estônia", envolvendo hackers patrióticos russos (CHIVVIS; DION-SCHWARZ, 2017).

Além da atribuição, outra questão fundamental para a segurança cibernética dos Estados são as vulnerabilidades estruturais. Nye (2010) adverte que a crescente dependência de sistemas digitais para atividades militares e econômicas abre novas brechas exploráveis por atores não estatais. Tais vulnerabilidades atingem especialmente as infraestruturas críticas, definidas pelo USA Patriot Act (2001) como sistemas e ativos, físicos ou virtuais, cuja destruição comprometeria a segurança nacional, a economia e a saúde pública dos Estados Unidos. Willett (2019) cita exemplos de setores visados por ataques, como bancos, indústrias petrolíferas, usinas nucleares, redes elétricas e sistemas de comunicação. Quanto maior a integração desses setores ao ciberespaço, maior a exposição a riscos.

O *Strategic Survey 2018*, do IISS (2018), introduz o conceito de "paradoxo da conectividade", segundo o qual os países mais tecnologicamente avançados são, paradoxalmente, os mais vulneráveis a

ataques cibernéticos. McCarthy et al. (2009, p. 545) reforçam essa ideia ao destacar que o ciberespaço funciona como o "sistema nervoso das infraestruturas críticas nacionais e da economia global". Nos Estados Unidos, por exemplo, um ataque a essas estruturas poderia provocar impactos catastróficos em múltiplas esferas: romper barragens e causar inundações, comprometer dados militares e de inteligência, ou ainda desestabilizar o sistema financeiro.

Muitos desses ataques empregam bombas lógicas — códigos maliciosos ocultos em falhas dos sistemas que são ativados estrategicamente em momentos de conflito (CLARKE; KNAKE, 2015). Essas bombas, além de danosas, servem como mecanismos de dissuasão, por meio da ameaça de retaliação severa. A detecção dessas ameaças, porém, é extremamente complexa: segundo dados do IISS (2018), o tempo médio de identificação pode ultrapassar 146 dias nos EUA e mais de 400 dias na União Europeia. Clarke e Knake (2015) apontam a vulnerabilidade da rede elétrica americana como exemplo emblemático, mencionando que, desde os anos 1990, a digitalização dos sistemas de controle facilita a sabotagem remota, como o aumento da rotação de geradores até a destruição de suas turbinas.

Adicionalmente, Gartzke (2013) observa que, embora as forças armadas americanas tenham se beneficiado do avanço tecnológico no campo de batalha, essa modernização também as tornou mais suscetíveis a ataques cibernéticos. Essa dualidade exemplifica os riscos intrínsecos à interdependência digital.

Outro desafio central reside no risco de escalada de tensões no ciberespaço, muitas vezes agravado pela falta de atribuição clara. Estratégias de contenção, nesse contexto, tornam-se cruciais. Nocetti (2018) relata, por exemplo, a abordagem cautelosa do governo Obama diante do roubo de dados do JP Morgan (2014) e do vazamento de informações da Casa Branca e do Departamento de Estado (2015). Apesar dos indícios apontarem hackers russos, possivelmente com respaldo do Kremlin, o governo evitou acusações diretas, optando por deixar que a mídia divulgasse os fatos, enviando assim uma mensagem política indireta.

O ciberespaço também está transformando profundamente as práticas de inteligência dos Estados. Um novo panorama se delineia com o crescimento de empresas privadas especializadas em cibersegurança, que atuam na detecção e análise de programas espiões. Essas empresas frequentemente publicam suas descobertas, democratizando o acesso à informação sobre as capacidades de espionagem digital dos governos. Essa nova realidade contrasta com o sigilo característico das operações durante a Guerra Fria (NOCETTI, 2018).

Como resultado dessa maior transparência, uma variedade de incidentes cibernéticos se torna objeto de análise pública e acadêmica, contribuindo para o amadurecimento do campo da segurança cibernética e oferecendo lições fundamentais sobre os riscos, estratégias e implicações políticas dos conflitos no espaço digital.

2.3 OPORTUNIDADES

No plano econômico, a segurança cibernética representa uma oportunidade de crescimento para setores especializados, como as empresas de tecnologia da informação, análise de risco, forense digital, criptografia e desenvolvimento de softwares de proteção. A demanda por soluções inovadoras em segurança digital estimula o empreendedorismo e a pesquisa científica, além de promover a criação de empregos altamente qualificados. A formação de profissionais capacitados para atuar em áreas como engenharia de segurança da informação, auditoria de sistemas e resposta a incidentes torna-se estratégica para os países que desejam se manter competitivos e proteger sua soberania digital. (SINGER; FRIEDMAN, 2014; NOCETTI, 2018)

No campo das relações internacionais, a segurança cibernética possibilita a construção de parcerias multilaterais, tratados de cooperação e mecanismos de governança global para lidar com ameaças comuns. Iniciativas como o desenvolvimento de marcos legais internacionais para o uso ético do ciberespaço, o intercâmbio de informações entre agências e a criação de protocolos de resposta conjunta a ciberataques fortalecem a diplomacia e a estabilidade internacional. Além disso, a cibersegurança promove o conceito de resiliência digital, ou seja, a capacidade dos sistemas e das sociedades de resistirem, responderem e se adaptarem rapidamente a ataques ou falhas tecnológicas, garantindo a continuidade dos serviços e a proteção dos direitos fundamentais dos cidadãos. (SINGER; FRIEDMAN, 2014; NOCETTI, 2018)

Do ponto de vista social, investir em segurança cibernética é uma forma de ampliar a confiança na utilização das tecnologias digitais. Ao garantir a privacidade dos dados, proteger sistemas de saúde, educação e finanças, e combater fraudes e desinformação, a cibersegurança contribui para a inclusão digital e para o fortalecimento da cidadania no ambiente virtual. Iniciativas de educação digital, campanhas de conscientização sobre práticas seguras e inclusão da cibersegurança nos currículos escolares e universitários representam importantes oportunidades de formação crítica da população frente aos desafios da sociedade da informação. (SINGER; FRIEDMAN, 2014; NOCETTI, 2018)

Portanto, embora os desafios da segurança cibernética sejam significativos, suas oportunidades são igualmente amplas. Elas envolvem não apenas avanços tecnológicos, mas também melhorias na governança pública, no desenvolvimento socioeconômico e na promoção de uma cultura digital segura e consciente. Aproveitar essas oportunidades exige planejamento, investimento e cooperação entre os setores público, privado e a sociedade civil, com vistas a construir um ciberespaço mais confiável, resiliente e inclusivo.

3 CONCLUSÃO

Diante do cenário apresentado ao longo deste trabalho, é possível afirmar que a segurança cibernética se consolidou como uma das principais questões da contemporaneidade, exigindo atenção estratégica de governos, empresas e da sociedade civil. Os desafios identificados, como o problema da

atribuição de ataques, as vulnerabilidades das infraestruturas críticas, a sofisticação crescente das ameaças e a possibilidade de escalada de conflitos entre Estados, evidenciam a complexidade do tema e sua interconexão com dimensões políticas, econômicas e sociais. A análise realizada demonstrou que a atuação no ciberespaço ultrapassa os limites do campo técnico, abrangendo também o âmbito da diplomacia, da segurança nacional e das relações internacionais, tornando-se essencial à manutenção da estabilidade e da soberania dos Estados.

Contudo, o estudo revelou também que, paralelamente aos riscos e ameaças, a segurança cibernética representa um campo fértil para oportunidades. O fortalecimento das estruturas de defesa digital pode impulsionar a inovação tecnológica, fomentar o crescimento de novos mercados e ampliar as possibilidades de cooperação internacional em torno de uma governança digital ética e responsável. A expansão de setores especializados, como forense digital, auditoria de sistemas, criptografia e desenvolvimento de softwares de proteção, abre novas frentes de atuação profissional e acadêmica, além de contribuir para a construção de uma cultura digital baseada na proteção de dados, na privacidade e na confiança dos usuários.

Além disso, observou-se que as iniciativas voltadas à educação e à conscientização da população sobre boas práticas no uso das tecnologias são fundamentais para reduzir a exposição a riscos, garantir o exercício pleno da cidadania no ambiente digital e promover a inclusão digital. Nesse contexto, a segurança cibernética deixa de ser uma responsabilidade exclusiva do Estado ou de especialistas em tecnologia e passa a demandar o envolvimento de múltiplos atores sociais. O fortalecimento da resiliência digital, por meio de investimentos em infraestrutura segura, marcos regulatórios atualizados e formação profissional adequada, torna-se indispensável para enfrentar os desafios emergentes e aproveitar, de forma estratégica, as oportunidades oferecidas pelo ambiente digital.

Por fim, é importante destacar que a consolidação de uma cultura de segurança cibernética também passa pela articulação entre as esferas pública e privada, pelo incentivo à pesquisa interdisciplinar e pela formulação de políticas públicas baseadas em evidências. A promoção da cooperação regional e internacional, a padronização de normas e protocolos de segurança e a criação de redes colaborativas de resposta a incidentes são estratégias fundamentais para a construção de um ecossistema digital mais seguro. Assim, enfrentar os desafios da cibersegurança com eficácia requer uma abordagem integrada, que valorize tanto a proteção técnica quanto os aspectos sociais, educacionais e éticos envolvidos na relação da sociedade com as tecnologias digitais.

Considerando o ritmo acelerado das transformações tecnológicas, é indispensável que os Estados e instituições estejam atentos à constante atualização de suas políticas e estratégias de segurança cibernética. A antecipação de riscos, a adoção de tecnologias emergentes como a inteligência artificial e o fortalecimento de capacidades locais de inovação são elementos-chave para garantir a soberania digital e a segurança da informação. Dessa forma, a segurança cibernética deve ser tratada como uma prioridade

permanente das agendas governamentais e institucionais, assegurando não apenas a proteção frente às ameaças, mas também o aproveitamento pleno das oportunidades trazidas pela era digital.

REFERÊNCIAS

OCDE. *Cybersecurity Policy Making at a Turning Point*. 2012. Disponível em: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf. Acesso em: 27 Jun.2025.

LE DRIAN, Jean-Yves. Discurso na 72ª Assembleia Geral da ONU, setembro de 2017. JUNCKER, Jean-Claude. Discurso sobre o estado da União. 2017.

NYE, Joseph S. *Cyber Power*. Cambridge: Belfer Center for Science and International Affairs, 2010.

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES (IISS). *Strategic Survey 2018: The Annual Assessment of Geopolitics*. Londres: IISS, 2018.

BOER, M.; VAZQUEZ, J. Cyber Security & Financial Stability: how cyber-attacks could materially impact the global financial system. Institute of International Finance, set. 2017. Disponível em: https://www.iif.com/Publications/ID/228/Cyber-Security- Financial-Stability-How-Cyber-attacks-Could-Materially-Impact-the-Global-Financial- System. Acesso em: 27 Jun.2025.

LLOYD'S OF LONDON. Estimativas de perdas financeiras devido a ciberataques. Julho de 2017.

WORLD ECONOMIC FORUM. *Global Risks Report 2018*. Genebra: WEF, 2018. Disponível em: https://www.weforum.org/reports/the-global-risks-report-2018. Acesso em: 27 Jun.2025.

SINGER, P. W.; FRIEDMAN, A. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Nova Iorque: Oxford University Press, 2014.

NOCETTI, J. *Géopolitique de la cyber-conflictualité*. Politique étrangère, vol. 83, n. 2, ver. 2018. Disponível em: https://www.ifri.org/fr/publications/politique- etrangere/articles-de-politique-etrangere/geopolitique-de-cyber. Acesso em: 27 Jun.2025.

GARTZKE, E. The Myth of Cyberwar: bringing war in cyberspace back down to Earth. *International Security*, Cambridge, v. 38, n. 2, p. 41-73, out. 2013. Disponível em: https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136. Acesso em: 27 Jun.2025.

FERNANDES, J. P. T. A ciberguerra como nova dimensão dos conflitos do século XXI. *Relações Internacionais*, Lisboa, n. 33, p. 53-69, mar. 2012. Disponível em: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1645-91992012000100005&lng=pt&nrm=iso. Acesso em: 27 Jun.2025.

CHIVVIS, C. S.; DION-SCHWARZ, C. Why It's So Hard to Stop a Cyberattack – and Even Harder to Fight Back. RAND Corporation, 2017. Disponível em: https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even- harder.html. Acesso em: 27 Jun.2025.

NYE, J. S. *Cyber War and Peace*. 2012. Disponível em: https://www.belfercenter.org/publication/cyber-war-and-peace. Acesso em: 27 Jun.2025.

USA PATRIOT ACT. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. Public Law 107-56 – Oct. 26, 2001. Disponível em: https://www.congress.gov/107/plaws/publ56/PLAW- 107publ56.pdf. Acesso em: 27 Jun.2025.

WILLETT, M. Cyber instruments and international security. The International Institute for Strategic Studies, 2019. Disponível em: https://www.iiss.org/blogs/analysis/2019/03/cyber-instruments-and-international- security. Acesso em: 27 Jun.2025

MCCARTHY, J. A.; BURROW, C.; DION, M.; PACHECO, O. Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Ed.). *Cyberpower and National Security*. 1. ed. Potomac Books, 2009. Cap. 23.

CLARKE, R.; KNAKE, R. *Cyber War: The Next Threat to National Security and What to Do About It*. Rio de Janeiro: Brasport, 2015.

GARTZKE, E. The Myth of Cyberwar: bringing war in cyberspace back down to Earth. *International Security*, Cambridge, v. 38, n. 2, p. 41-73, out. 2013. Disponível em: https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136. Acesso em: 27 Jun.2025