ISBN: 978-65-986235-3-1

Aurum EDITORA

CAPÍTULO 17

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA: DESAFIOS E SOLUÇÕES NO SÉCULO XXI

THE EVOLUTION OF CYBER SECURITY: CHALLENGES AND SOLUTIONS IN THE 21ST CENTURY

https://doi.org/10.63330/aurumpub.005-017

David Aguiar
Segurança Cibernética

RESUMO

Este trabalho de conclusão de curso tem como tema central a evolução da segurança cibernética no século XXI, com ênfase nos principais desafios enfrentados por indivíduos, organizações e governos, bem como nas soluções desenvolvidas para mitigar os riscos no ambiente digital. Considerando o avanço exponencial da tecnologia, a crescente dependência de sistemas informacionais e a sofisticação dos crimes cibernéticos, torna-se essencial compreender como a cibersegurança se transformou em uma pauta estratégica em escala global. O objetivo geral da pesquisa foi analisar criticamente a evolução da segurança cibernética, identificando as principais ameaças contemporâneas, como ataques de ransomware, invasões de sistemas, vulnerabilidades em dispositivos da Internet das Coisas (IoT) e a fragilidade das legislações frente às novas formas de criminalidade digital. Para isso, foi adotada uma metodologia qualitativa, de natureza exploratória, com base em revisão bibliográfica e documental. Foram consultadas obras acadêmicas, relatórios técnicos, discursos políticos e estudos especializados de autores e instituições reconhecidas na área, como Doneda (2019), Bauman (2017), Castells (2003), Anderson e Moore (2020), além de organismos como a OCDE, IBM, Fórum Econômico Mundial e o International Institute for Strategic Studies. A pesquisa foi estruturada em três capítulos principais. No primeiro, desenvolve-se um panorama histórico e conceitual da segurança cibernética, desde seus primórdios até a sua consolidação como prioridade na governança digital. No segundo capítulo, são discutidos os desafios técnicos, organizacionais, jurídicos e sociais da cibersegurança no contexto atual, com destaque para a descentralização do trabalho, a defasagem regulatória e a insuficiência de cultura de segurança em ambientes corporativos. Também são analisadas as soluções implementadas, como o modelo Zero Trust, a criptografia avançada, o uso de inteligência artificial para detecção de ameaças e a importância da cooperação internacional. O terceiro capítulo apresenta a síntese dos principais achados, destacando a complexidade do cenário e a necessidade de abordagens interdisciplinares e colaborativas. Conclui-se que a segurança cibernética não pode mais ser tratada apenas como uma questão técnica, mas como um desafio transversal que demanda integração entre tecnologia, legislação, educação, governança e políticas públicas. A proteção do ciberespaço exige ações coordenadas em nível local e global, que visem não apenas à defesa dos sistemas, mas à preservação dos direitos, da privacidade e da confiança social na era digital.

Palavras-chave: Segurança Cibernética; Crimes Digitais; Proteção de Dados; Tecnologias da Informação.

ABSTRACT

The central theme of this term paper is the evolution of cybersecurity in the 21st century, with an emphasis on the main challenges faced by individuals, organizations and governments, as well as the solutions developed to mitigate risks in the digital environment. Considering the exponential advance of technology, the growing dependence on information systems and the sophistication of cybercrime, it is essential to understand how cybersecurity has become a strategic agenda on a global scale. The general objective of the research was to critically analyze the evolution of cybersecurity, identifying the main contemporary threats,

such as ransomware attacks, system invasions, vulnerabilities in Internet of Things (IoT) devices and the fragility of legislation in the face of new forms of digital crime. To this end, a qualitative, exploratory methodology was adopted, based on a bibliographic and documentary review. We consulted academic works, technical reports, political speeches and specialized studies by renowned authors and institutions in the field, such as Doneda (2019), Bauman (2017), Castells (2003), Anderson and Moore (2020), as well as organizations such as the OECD, IBM, the World Economic Forum and the International Institute for Strategic Studies. The research is structured in three main chapters. The first provides a historical and conceptual overview of cybersecurity, from its beginnings to its consolidation as a priority in digital governance. The second chapter discusses the technical, organizational, legal and social challenges of cybersecurity in the current context, highlighting the decentralization of work, the regulatory gap and the lack of a security culture in corporate environments. Implemented solutions are also analyzed, such as the Zero Trust model, advanced cryptography, the use of artificial intelligence to detect threats and the importance of international cooperation. The third chapter summarizes the main findings, highlighting the complexity of the scenario and the need for interdisciplinary and collaborative approaches. It concludes that cyber security can no longer be treated solely as a technical issue, but as a cross-cutting challenge that demands integration between technology, legislation, education, governance and public policies. Protecting cyberspace requires coordinated action at local and global level, aimed not only at defending systems, but also at preserving rights, privacy and social trust in the digital age.

Keywords: Cyber Security; Digital Crimes; Data Protection; Information Technology.

1 INTRODUÇÃO

A crescente digitalização das estruturas sociais, econômicas e políticas no século XXI tem gerado transformações profundas no modo como indivíduos, instituições e Estados se organizam e interagem. A segurança cibernética, nesse contexto, torna-se uma preocupação central, uma vez que os riscos associados ao uso indevido de informações, invasões de sistemas e crimes digitais complexos crescem na mesma proporção em que a tecnologia se expande e se integra ao cotidiano. Esse cenário, caracterizado por um ambiente global interconectado e tecnologicamente dependente, impõe desafios sem precedentes à proteção de dados, à soberania informacional e à preservação dos direitos fundamentais. Segundo autores como Castells (2003) e Bauman (2017), vivemos uma era de redes fluidas e fronteiras digitais frágeis, em que a segurança se redefine constantemente diante das ameaças emergentes.

Diante disso, o presente Trabalho de Conclusão de Curso tem como objetivo principal analisar a evolução da segurança cibernética nas últimas décadas, com ênfase nos desafios enfrentados por diferentes setores da sociedade e nas soluções propostas e adotadas para mitigar os riscos no ambiente digital. Parte-se da hipótese de que, apesar dos avanços tecnológicos e normativos já implementados, as ações isoladas são insuficientes para garantir uma cibersegurança eficaz; sendo necessário um modelo multidisciplinar que una tecnologia, legislação, cooperação internacional, educação e governança estratégica. A escolha do tema justifica-se por sua atualidade, relevância global e impacto direto na vida das pessoas e na estabilidade das instituições, especialmente em contextos marcados por ameaças persistentes, como ataques de ransomware, espionagem digital e manipulação de dados sensíveis.

A metodologia adotada para a elaboração deste trabalho baseia-se em uma abordagem qualitativa e exploratória, fundamentada em pesquisa bibliográfica e documental. Foram consultadas obras clássicas e contemporâneas sobre o tema, com destaque para autores como Doneda (2019), Nye (2011), Rezende (2020), Anderson e Moore (2020), Ferreira e Almeida (2021) e Zúquete (2022), além de relatórios técnicos de instituições renomadas, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2012), o Fórum Econômico Mundial (2018), a IBM Security (2024), o Lloyd's of London (2017) e o International Institute for Strategic Studies (2018). A seleção das fontes seguiu critérios de relevância acadêmica e atualidade, buscando oferecer uma visão ampla e fundamentada sobre os principais aspectos da segurança cibernética contemporânea. O procedimento metodológico incluiu a leitura, sistematização e análise crítica das publicações, permitindo a identificação de padrões, desafios recorrentes e propostas inovadoras.

A estrutura do trabalho está dividida em três partes interdependentes. O primeiro capítulo trata da contextualização teórica e histórica da segurança cibernética, abordando desde o surgimento das preocupações digitais no final do século XX até sua consolidação como pauta estratégica no século XXI. São discutidos os impactos da revolução informacional e da dependência tecnológica no surgimento de novas

ameaças e na reorganização dos mecanismos de segurança em nível global. O segundo capítulo concentra-se na análise dos principais desafios enfrentados pela cibersegurança atualmente, tais como ataques sofisticados, vulnerabilidades de dispositivos conectados (IoT), descentralização das estruturas de trabalho, defasagem legislativa e falta de cultura organizacional de segurança. Também são discutidas as soluções implementadas e em desenvolvimento, como o modelo "Zero Trust", o uso de criptografia avançada, inteligência artificial aplicada à defesa digital, políticas de compliance e ações de cooperação internacional.

O terceiro e último capítulo apresenta as considerações finais da pesquisa, com a síntese dos principais achados e uma reflexão crítica sobre as tendências futuras da segurança cibernética. Reforça-se a necessidade de uma abordagem transversal, que envolva múltiplos atores e dimensões — técnica, jurídica, institucional e cultural — para que se possa enfrentar com eficácia os desafios complexos do ciberespaço.

Com essa estrutura, o trabalho pretende não apenas descrever os avanços e obstáculos da cibersegurança no século XXI, mas também contribuir para o debate acadêmico e institucional sobre as formas mais adequadas de proteger o ambiente digital, os dados dos cidadãos e os sistemas críticos de informação em uma era cada vez mais vulnerável e interdependente.

2 DESENVOLVIMENTO

2.1 SEGURANÇA CIBERNÉTICA

A Segurança da Informação é uma disciplina relativamente recente no âmbito do conhecimento humano, mas que ganhou destaque significativo nas últimas décadas devido ao crescimento exponencial do uso da tecnologia. Para Araujo e Ferreira (2009), trata-se de uma área essencial que exige a elaboração e implementação de políticas eficazes, especialmente voltadas à proteção da confidencialidade das informações. Os autores propõem um guia prático para políticas de segurança, classificando os sistemas de informação em níveis de acesso e controle — do mais restrito ao mais básico. Entretanto, eles reconhecem que os demais princípios da segurança da informação, como integridade e disponibilidade, ainda carecem de maior aprofundamento.

Complementando essa perspectiva, Fontes (2006) apresenta a segurança da informação com ênfase no papel do usuário, adotando uma abordagem organizacional. Para ele, é fundamental investir na preparação e conscientização dos usuários, pois a manipulação inadequada dos dados pode comprometer toda a estrutura de segurança. Seu enfoque na educação do usuário busca garantir que as informações sejam tratadas com responsabilidade, promovendo assim um ambiente digital mais seguro.

Nesse mesmo sentido, o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), por meio de sua cartilha educativa, oferece orientações práticas sobre os principais riscos enfrentados pelos usuários da internet. A cartilha descreve golpes, ataques e vulnerabilidades

recorrentes, ao mesmo tempo em que apresenta ferramentas e boas práticas para utilizar a internet de forma segura.

Laudon e Laudon (2014), por sua vez, destacam que compreender os sistemas de informação é vital para o fortalecimento de empresas competitivas, a gestão de corporações globais e o fornecimento de serviços e produtos úteis. Em sua obra, os autores abordam os sistemas de informação de forma prática e didática, com exemplos reais e abordagem ética, enfatizando a importância da privacidade e da segurança digital no contexto empresarial.

Spyman (2000) trata de um tema polêmico, mas necessário: o surgimento de hackers e a vulnerabilidade de empresas e usuários conectados à internet. Em *Manual Completo Hacker Millennium*, o autor apresenta os principais nomes e terminologias do universo hacker, explicando suas motivações, métodos e como evitá-los. A obra também oferece uma introdução aos programas e scripts disponíveis na internet, revelando como eles podem ser utilizados de maneira ofensiva ou defensiva.

No campo jurídico, Clough (2010) analisa os princípios do cibercrime sob a perspectiva de diferentes jurisdições — Austrália, Canadá, Reino Unido e Estados Unidos. Sua obra é um marco para aqueles que buscam compreender os desafios legais e investigativos relacionados ao crime cibernético, trazendo exemplos práticos e análises comparativas entre os sistemas jurídicos.

Nesse sentido, Gragido et al. (2013) oferecem uma abordagem especializada sobre segurança cibernética, investigando as ações de organizações criminosas virtuais, a espionagem industrial e os impactos econômicos e geopolíticos dos crimes cibernéticos. Os autores reúnem suas expertises para construir uma verdadeira enciclopédia sobre ameaças digitais, abordando desde ataques coordenados por Estados até as chamadas guerras cibernéticas.

Ao se discutir crimes cibernéticos, é importante diferenciar os cibercrimes dos chamados crimes de informática. Os crimes de informática englobam qualquer conduta ilegal relacionada ao processamento de dados, seja na forma de armazenamento, compilação ou transmissão. Já o cibercrime, de modo mais específico, diz respeito a delitos cometidos por meio da tecnologia da informação com o objetivo de causar dano a terceiros. Tais condutas ilícitas podem ser enquadradas legalmente como crimes virtuais, já tipificados pelo Código Penal Brasileiro.

Schmidt (2014) classifica os crimes cibernéticos em três categorias principais: crimes puros, mistos e comuns. Os crimes puros afetam diretamente a estrutura física (hardware) ou lógica (software) de sistemas computacionais, como no caso do vírus Melissa, que em 1999 gerou prejuízos superiores a 80 milhões de dólares ao comprometer usuários do Microsoft Word. Os crimes mistos utilizam a tecnologia como meio para a execução da ação criminosa, como nas fraudes por meio de Internet Banking. Já os crimes comuns se valem da internet apenas como canal para a disseminação do conteúdo ilícito, como ocorre nos casos de pornografia infantil.

Ainda segundo Schmidt (2014), os crimes cibernéticos podem ser classificados em próprios, quando o alvo e a ferramenta do crime são ambos sistemas computacionais — como em invasões de rede realizadas por hackers —, e impróprios, quando o computador é apenas um meio para atingir vítimas humanas ou instituições, a exemplo de casos de estelionato, calúnia ou pedofilia digital.

A crescente sofisticação desses crimes reforça a importância da cibersegurança como um dos principais temas da agenda internacional contemporânea. Até o final do século XX, as principais preocupações de segurança estavam voltadas a conflitos armados, à segurança humana e ao meio ambiente. No entanto, com a virada do milênio, a cibersegurança emerge como novo eixo estratégico, impulsionada pela revolução informacional e pela aceleração da transformação digital.

O relatório da Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2012) evidenciou a centralidade da internet para o desenvolvimento econômico e social, bem como o aumento das ameaças digitais. Essa preocupação foi reiterada por líderes como Jean-Yves Le Drian e Jean-Claude Juncker, que alertaram para os riscos à liberdade, à democracia e à estabilidade institucional decorrentes de ataques cibernéticos. Nye (2018) destaca que, desde 2013, os riscos digitais passaram a ser considerados a maior ameaça à segurança nacional dos Estados Unidos, visão corroborada pelo *Strategic Survey* do International Institute for Strategic Studies (IISS, 2018), que reconhece o impacto da revolução digital sobre todas as formas de governança global.

No campo econômico, os prejuízos são alarmantes. Boer e Vazquez (2017) apontam que um ataque cibernético em larga escala pode gerar perdas superiores a 121 bilhões de dólares. O *Global Risks Report* do Fórum Econômico Mundial (2018) estima que, entre 2017 e 2022, o custo global do cibercrime para as empresas pode atingir 8 trilhões de dólares.

Diante desse panorama, torna-se evidente que compreender o funcionamento do ciberespaço e enfrentar os desafios da cibersegurança é essencial para a formulação de políticas eficazes e para a proteção de indivíduos, empresas e governos frente aos riscos da era digital.

2.2 DESAFIOS E SOLUÇÕES NO SÉCULO XXI

A segurança cibernética tornou-se um dos maiores desafios do século XXI, impulsionada pela crescente digitalização de dados, serviços e relações sociais, bem como pela rápida transformação tecnológica que caracteriza a chamada Quarta Revolução Industrial. À medida que governos, empresas e indivíduos migram suas atividades para o ambiente digital, aumentam também as ameaças cibernéticas, que se tornam cada vez mais complexas, organizadas e difíceis de combater. Como destacam Castells (2003) e Bauman (2017), vivemos em uma era marcada pela fluidez das redes, pela interconectividade global e pela fragilidade das fronteiras digitais, o que amplia significativamente os riscos para a integridade, confidencialidade e disponibilidade das informações.

Um dos principais desafios da segurança cibernética contemporânea reside na sofisticação dos ataques. Grupos criminosos e ciberatacantes utilizam técnicas avançadas, como phishing com engenharia social refinada, ataques de ransomware, exploração de vulnerabilidades em sistemas legados, e a utilização de inteligência artificial para automatizar ataques em larga escala. Segundo relatório da IBM Security (2024), o tempo médio de detecção de uma violação de dados ainda ultrapassa 200 dias, o que demonstra a vulnerabilidade estrutural das organizações diante de ameaças persistentes e ocultas.

Além disso, o crescimento da Internet das Coisas (IoT) e da computação em nuvem introduziu novas superfícies de ataque. Cada dispositivo conectado representa uma possível brecha na rede, especialmente em contextos nos quais a segurança embarcada é negligenciada por questões de custo ou agilidade de mercado. Conforme observa Zúquete (2022), a fragmentação e heterogeneidade dos dispositivos conectados dificultam a implementação de políticas unificadas de proteção e monitoramento.

Outro desafio emergente é o da cibersegurança em ambientes de trabalho remoto, intensificado pela pandemia da COVID-19. Com a descentralização dos espaços corporativos, os perímetros tradicionais de segurança foram diluídos, exigindo novas abordagens, como o modelo "Zero Trust", que parte do princípio de que nenhuma entidade — interna ou externa — deve ser automaticamente confiável. Conforme ressaltam Ferreira e Almeida (2021), essa mudança de paradigma exige uma reestruturação profunda das práticas de autenticação, autorização e monitoramento.

No campo jurídico e regulatório, o desafio é igualmente significativo. A lentidão da legislação em acompanhar as rápidas mudanças tecnológicas gera lacunas legais, dificultando a responsabilização de cibercriminosos e a definição de limites claros sobre o uso ético dos dados. A promulgação da Lei Geral de Proteção de Dados (LGPD), no Brasil, e do Regulamento Geral de Proteção de Dados (GDPR), na União Europeia, representa avanços importantes, mas ainda insuficientes diante da globalização das ameaças. Como observa Doneda (2019), a proteção de dados exige não apenas normas, mas uma cultura de responsabilidade digital e transparência.

Em resposta a esses desafios, diversas soluções têm sido propostas e implementadas em múltiplos níveis. No plano técnico, destacam-se o uso crescente de criptografia de ponta a ponta, o desenvolvimento de algoritmos de detecção de anomalias com base em machine learning e a adoção de firewalls inteligentes que se atualizam em tempo real. As estratégias de defesa cibernética também passam a incorporar práticas proativas, como pentests, simulações de ataques e auditorias contínuas. Segundo Anderson e Moore (2020), a cibersegurança não deve ser pensada como um estado, mas como um processo contínuo de adaptação e resposta.

Do ponto de vista organizacional, o investimento em educação e cultura de segurança é fundamental. Funcionários despreparados representam uma das maiores vulnerabilidades, sendo responsáveis por uma parte considerável das brechas exploradas por atacantes. A capacitação contínua, associada a políticas claras

de uso dos sistemas e à conscientização sobre boas práticas digitais, torna-se uma estratégia essencial. Nesse sentido, Rezende (2020) aponta que a cibersegurança deve ser integrada ao planejamento estratégico das instituições, e não tratada apenas como uma função técnica do setor de TI.

No nível governamental e internacional, a cooperação entre países, agências reguladoras e empresas privadas é cada vez mais necessária para enfrentar ataques transnacionais. Iniciativas como a criação de centros de resposta a incidentes (CERTs), a assinatura de acordos multilaterais e a atuação conjunta de forças policiais especializadas têm mostrado resultados promissores. Contudo, ainda existem barreiras geopolíticas e interesses econômicos que dificultam ações coordenadas em larga escala. Como lembra Nye (2011), o ciberespaço é um território novo onde o poder é difuso, e a soberania nacional se vê constantemente desafiada por atores não estatais e transnacionais.

Dessa forma, a segurança cibernética no século XXI é um campo em constante transformação, que exige um olhar multidisciplinar, reunindo conhecimentos de tecnologia, direito, administração, ética e educação. O enfrentamento dos desafios cibernéticos passa, inevitavelmente, por soluções integradas e colaborativas, capazes de proteger não apenas sistemas e dados, mas os próprios valores democráticos e a confiança social na era digital.

3 CONCLUSÃO

Diante da complexidade e da abrangência do tema estudado, conclui-se que a segurança cibernética constitui hoje uma das mais urgentes e estratégicas preocupações da sociedade contemporânea, impactando diretamente os setores público, privado e civil em escala global. A pesquisa demonstrou que, à medida que as tecnologias digitais se tornaram onipresentes na vida social, econômica e institucional, os riscos associados ao ciberespaço evoluíram em sofisticação, frequência e impacto. Essa nova realidade exige não apenas a adoção de ferramentas técnicas de proteção, mas uma abordagem sistêmica, multidisciplinar e preventiva, capaz de articular soluções jurídicas, organizacionais, educacionais e políticas. A elemento estruturante para a soberania digital, a proteção dos direitos fundamentais, a estabilidade econômica e a confiança social. Ela está diretamente relacionada à proteção da privacidade, à liberdade de expressão, à integridade das instituições democráticas e ao bem-estar dos cidadãos em um mundo cada vez mais digitalizado. A evolução da cibersegurança deve, portanto, acompanhar o ritmo da inovação tecnológica, mas também das transformações sociais, culturais e normativas que permeiam o uso da informação.

Sendo assim, o presente trabalho contribui para o debate acadêmico e institucional ao reafirmar a necessidade de políticas públicas robustas, marcos regulatórios eficazes e práticas de gestão inovadoras voltadas à construção de um ambiente digital mais seguro, ético e resiliente. Conclui-se, portanto, que o fortalecimento da cibersegurança é um imperativo coletivo, contínuo e interdisciplinar, essencial para enfrentar os desafios do século XXI e garantir a integridade da sociedade da informação. Somente com

articulação entre conhecimento técnico, sensibilidade ética, visão estratégica e vontade política será possível proteger os sistemas, os dados e, sobretudo, as pessoas que habitam e dependem do universo digital em constante transformação.

REFERÊNCIAS

ANDERSON, Ross; MOORE, Tyler. *Security Economics and the Internal Market*. European Network and Information Security Agency – ENISA, 2020. Disponível em: https://www.enisa.europa.eu. Acesso em: 10 jul. 2025.

ARAUJO, Márcio T.; FERREIRA, Fernando Nicolau Freitas. *Política de Segurança da Informação*. 2. ed. –: Ciência Moderna, 2009.

BAUMAN, Zygmunt. *Vigilância líquida*. Rio de Janeiro: Zahar, 2017.

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: 14 jul. 2025.

CASTELLS, Manuel. *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Rio de Janeiro: Zahar, 2003.

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

CLOUGH, Jonathan. *Principles of Cybercrime*. New York: Cambridge University Press, 2010.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Thomson Reuters Brasil, 2019.

FERREIRA, Ana Paula; ALMEIDA, Lucas Henrique. Cibersegurança e o modelo Zero Trust: uma abordagem emergente frente ao trabalho remoto. *Revista Gestão e Tecnologia*, v. 21, n. 2, p. 132–148, 2021.

FONTES, Edison Luiz Gonçalves. *Segurança da Informação: o usuário faz a diferença*. Rio de Janeiro: Saraiva, 2007.

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: 14 jul. 2025.

GRAGIDO, Will; MOLINA, Daniel; PIRC, John; SELBY, Nick; HAY, Andrew. *Blackhatonomics: an inside look at the economics of cybercrime*. Waltham: Elsevier, 2013.

IBM SECURITY. *Cost of a Data Breach Report 2024*. Armonk, NY: IBM Corporation, 2024. Disponível em: https://www.ibm.com/security/data-breach. Acesso em: 10 jul. 2025.

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES (IISS). *Strategic Survey 2018: The Annual Assessment of Geopolitics*. Londres: IISS, 2018. JUNCKER, Jean-Claude. *Discurso sobre o estado da União*. 2017.

LAUDON, Kenneth; LAUDON, Jane. *Sistemas de Informações Gerenciais*. –: Pearson Universidades, 2014.

LE DRIAN, Jean-Yves. *Discurso na 72ª Assembleia Geral da ONU*, setembro de 2017.

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

NYE, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.

OCDE. *Cybersecurity Policy Making at a Turning Point*. 2012. Disponível em: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf. Acesso em: 14 jul. 2025.

REZENDE, Denis Alcides. *Governança de Tecnologia da Informação e Comunicação: fundamentos, modelos e aplicação nas organizações*. 3. ed. São Paulo: Atlas, 2020.

SCHMIDT, Guilherme. Crimes Cibernéticos. 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 14 jul. 2025.

SPYMAN, Hacking. *Manual Completo do Hacker*. 3. ed. –: Book Express, 2000.

WORLD ECONOMIC FORUM. *Global Risks Report 2018*. Genebra: WEF, 2018. Disponível em: https://www.weforum.org/reports/the-global-risks-report-2018. Acesso em: 14 jul. 2025.

ZÚQUETE, André. *Segurança em Redes e Sistemas Computacionais*. Lisboa: FCA, 2022.