JOIN: JOURNAL OF SOCIAL SCIENCE

https://ejournal.mellbaou.com/index.php/join/index

Open Access

Cite this article: Indi Nuroni, Eddy Sumartono, Darmawan Darmawan, Muhammad Asykur Muchtar, Johannes Johny Koynja, 2024. The Impact of Cybercrime on Global Security. Join: Journal of Social Science Vol.1(5) page 199-214

Keywords:
Cybercrime, Global Security, Cyber Security, Law

Author for correspondence:
Indi Nuroni
e-mail: nuroini.indi@gmail.com

Published by:

GLOBAL SOCIETY PUBLISHING

The Impact of Cybercrime on Global Security

[1]Indi Nuroni, [2]Eddy Sumartono, [3]Darmawan, [4]Muhammad Asykur Muchtar, [5]Johannes Johny Koynja

[1]Universitas Bhayangkara Surabaya, [2]Universitas Krisna Dwipayana (Unkris), Jakarta, [3]Yayasan Pendidikan Al - Khoeriyah Brebes, [4]Universitas Muhammadiyah Sorong, [5]Universitas Mataram, Indonesia

This study investigates the profound impact of cybercrime on global security, highlighting the multifaceted threats posed by cybercriminal activities to nations, businesses, and individuals worldwide. As digital technologies and internet connectivity expand, the frequency and sophistication of cybercrime have surged, posing significant risks to economic stability, national security, and public safety. Through a comprehensive literature review, this research examines various dimensions of cybercrime, including financial fraud, data breaches, cyber espionage, and critical infrastructure attacks. The findings reveal that cybercrime not only inflicts substantial economic losses but also undermines trust in digital systems, disrupts essential services, and compromises sensitive information. Furthermore, the study underscores the global nature of cyber threats, emphasizing that no country is immune to these risks, necessitating international cooperation and coordinated responses. The research also explores the effectiveness of current cybersecurity measures and policies, identifying gaps and suggesting improvements to enhance global cyber resilience. Key recommendations include the development of robust legal frameworks, advanced technological defenses, and comprehensive awareness programs to combat cyber threats. Additionally, the study highlights the importance of public-private partnerships and the role of international organizations in fostering a collective defense against cybercrime. By providing a holistic view of the impact of cybercrime on global security, this study offers valuable insights for policymakers, cybersecurity professionals, and scholars, advocating for a proactive and collaborative approach to safeguarding the digital landscape.

1. Introduction

Cybercrime has emerged as a critical threat to global security, affecting nations, organizations, and individuals alike. As digital technologies become increasingly integrated into everyday life, the reliance on the internet and networked systems has exposed vulnerabilities that cybercriminals exploit for financial gain, espionage, and disruption of services (Brenner, 2010). The impact of cybercrime extends beyond economic losses, as it also poses significant risks to national security, critical infrastructure, and public safety (Clarke & Knake, 2010). The global nature of cybercrime, with attacks often crossing multiple borders and jurisdictions, complicates efforts to combat these threats and requires a coordinated international response (Broadhurst, 2006). Despite the growing recognition of cybercrime as a major security challenge, the full scope and implications of its impact on global security remain underexplored.

The existing research on cybercrime primarily focuses on specific types of cyberattacks, such as ransomware, phishing, and data breaches, and their immediate consequences for targeted organizations (Sullivan et al., 2018). While these studies provide valuable insights into the tactics and techniques used by cybercriminals, there is a significant research gap in understanding the broader implications of cybercrime on global security. Most studies tend to examine cybercrime from a technological or legal perspective, often neglecting the geopolitical, economic, and social dimensions of cyber threats (Wall, 2007). Additionally, the rapidly evolving nature of cybercrime, driven by technological advancements and the increasing sophistication of attackers, necessitates continuous research to keep pace with emerging threats and develop effective countermeasures (Rid & Buchanan, 2015). This gap highlights the need for a more comprehensive analysis of cybercrime that considers its impact on global security from multiple angles.

The urgency of this research is underscored by the increasing frequency and severity of cyberattacks worldwide, which threaten to destabilize global security and disrupt critical infrastructure (Lewis, 2018). High-profile incidents, such as the WannaCry ransomware attack and the SolarWinds breach, have demonstrated the potential of cybercrime to cause widespread damage and undermine trust in digital systems (Guitton, 2017). Moreover, the COVID-19 pandemic has exacerbated cyber risks, as the shift to remote work and increased reliance on digital platforms have created new opportunities for cybercriminals to exploit (Buil-Gil et al., 2020). As nations and organizations grapple with these evolving threats, understanding the impact of cybercrime on global security is crucial for developing effective policies and strategies to mitigate risks and enhance resilience.

Previous studies have explored various aspects of cybercrime, such as its economic impact, legal challenges, and technical countermeasures (Anderson et al., 2013; Holt & Bossler, 2016). However, these studies often focus on isolated incidents or specific sectors, lacking a holistic view of how cybercrime affects global security across different contexts (Broadhurst, 2006). Recent research has begun to examine the strategic implications of cybercrime for national security, emphasizing the need for coordinated international efforts to combat cyber threats and protect critical infrastructure (Clarke & Knake, 2010; Rid & Buchanan, 2015). Yet, there remains a lack of comprehensive frameworks and empirical evidence to guide policymakers and security professionals in understanding the complex and multifaceted impact of cybercrime on global security. This study seeks to address these gaps by analyzing the broader implications of cybercrime on global security, drawing on insights from multiple disciplines and case studies.

The novelty of this research lies in its multidisciplinary approach to understanding the impact of cybercrime on global security. By integrating perspectives from cybersecurity, international relations, economics, and sociology, this study aims to provide a more comprehensive understanding of how cybercrime affects global security in diverse settings (Brenner, 2010). The primary objective of this research is to develop a framework for analyzing the impact of cybercrime on global security, highlighting key factors that influence the effectiveness of cybersecurity measures and identifying best practices for enhancing resilience against cyber threats. The findings are expected to contribute to the academic literature on cybercrime and global security and offer practical insights for policymakers, security professionals, and organizations seeking to navigate the complexities of the digital age.

2. Research Method

This study employs a qualitative research approach through a literature review to explore the impact of cybercrime on global security. A literature review is an appropriate method for this research as it allows for a comprehensive examination and synthesis of existing knowledge, theories, and empirical findings related to cybercrime and its implications for global security (Snyder, 2019). By systematically reviewing the literature, this study aims to identify key themes, trends, and gaps in the current understanding of how cybercrime affects global security across various dimensions, including technological, economic, geopolitical, and social aspects (Webster & Watson, 2002). This approach also provides a foundation for developing a conceptual framework that can guide future research and inform policy-making and strategic decision-making in cybersecurity.

The sources of data for this literature review consist of secondary data, including peer-reviewed journal articles, books, conference papers, government and industry reports, and other scholarly publications that focus on cybercrime and global security. These sources were selected from reputable academic databases such as JSTOR, Google Scholar, Web of Science, and Scopus to ensure the credibility and relevance of the information gathered (Cooper, 2010). The inclusion criteria for studies were that they must provide empirical evidence, theoretical insights, or case studies related to cybercrime, with a particular focus on its impact on global security, including threats to critical infrastructure, national security, and economic stability (Tranfield, Denyer, & Smart, 2003).

Data collection involved a systematic search of the literature using specific keywords such as "cybercrime," "global security," "cybersecurity," "critical infrastructure," "digital threats," and "international cyber policy." The search process identified a broad range of studies, which were then screened for inclusion based on their relevance, quality, and focus on the impact of cybercrime on global security. The selected literature was organized thematically to cover different dimensions of cybercrime and its implications, such as the economic costs of cybercrime, the role of state and non-state actors in cyberattacks, legal and regulatory challenges, and the strategies for enhancing cybersecurity at the national and international levels (Flick, 2014). This thematic organization enabled a structured analysis of the existing knowledge on cybercrime and its impact on global security.

For data analysis, this study employed thematic analysis, a qualitative method suitable for identifying, analyzing, and reporting patterns within the literature (Braun & Clarke, 2006). The analysis began with an initial coding of the literature to identify recurring themes and concepts related to the impact of cybercrime on global security. These codes were then grouped into broader themes that capture the various dimensions of cybercrime, such as economic impact, geopolitical implications, technological vulnerabilities, and international cooperation (Nowell et al., 2017). By synthesizing these themes, the study aimed to provide a comprehensive understanding of the impact of cybercrime on global security and to highlight areas where further research is needed. This approach not only contributes to the academic literature but also offers practical insights for policymakers, security professionals, and organizations seeking to enhance their cybersecurity posture and mitigate the risks associated with cybercrime.

3. Result and Discussion

3.1. Economic Impact of Cybercrime on Global Security

Cybercrime has significant economic implications, which are a major concern for global security. The financial losses associated with cybercrime have been escalating rapidly, affecting individuals, corporations, and governments worldwide (Anderson et al., 2013). Estimates suggest that cybercrime costs the global economy billions of dollars annually, with the damages including stolen assets, business disruption, and the costs of response and recovery efforts (Lewis, 2018). For instance, ransomware attacks have become increasingly prevalent, targeting critical infrastructure and demanding substantial ransoms, which can lead to severe economic disruptions and threaten national security (Guitton, 2017). These financial impacts not only burden economies but also undermine public trust in digital systems and the broader digital economy.

Moreover, the economic impact of cybercrime extends beyond direct financial losses. Indirect costs, such as reputational damage, loss of consumer confidence, and decreased stock market valuations, can be substantial (Sullivan et al., 2018). Companies that suffer data breaches or cyberattacks often face a loss of customer trust, which can have long-term effects on their market position and profitability (Ponemon Institute, 2019). Additionally, the need for increased investment in cybersecurity measures, insurance, and legal fees further strains resources, diverting funds from innovation and growth (Brenner, 2010). These economic impacts demonstrate the interconnected nature of cybersecurity and economic stability, emphasizing the need for robust cybersecurity measures to protect the global economy.

The economic impact of cybercrime also highlights disparities in cybersecurity readiness and resilience across different regions and sectors (Clarke & Knake, 2010). Developing countries and small businesses often lack the resources and expertise needed to defend against sophisticated cyber threats, making them particularly vulnerable to economic disruption caused by cybercrime (Broadhurst, 2006). This vulnerability is exacerbated by the global nature of cybercrime, where attacks can originate from anywhere and target multiple jurisdictions simultaneously. As a result, cybercrime poses a unique challenge to global security, requiring coordinated international efforts to build capacity, share information, and develop effective countermeasures (Rid & Buchanan, 2015).

In conclusion, the economic impact of cybercrime is a critical aspect of its threat to global security. The financial losses and broader economic disruptions caused by cybercrime underscore the importance of robust cybersecurity strategies and international cooperation to mitigate these risks. By understanding the economic dimensions of cybercrime, policymakers and security professionals can develop more targeted and effective responses to protect global security and economic stability.

Cybercrime has a profound economic impact on global security, affecting individuals, businesses, and governments worldwide. The financial losses attributed to cybercrime are staggering, with estimates suggesting that the global economy loses billions of dollars annually due to cyber attacks (Anderson et al., 2013).

These losses arise from a variety of cybercriminal activities, including data breaches, ransomware attacks, and intellectual property theft. The economic damage caused by these activities extends beyond direct financial losses, encompassing costs associated with recovery efforts, regulatory fines, legal fees, and the loss of consumer trust (Lewis, 2018). For instance, ransomware attacks that disrupt critical infrastructure or business operations can lead to significant economic disruptions, threatening the stability and functionality of affected organizations and sectors (Guitton, 2017).

Moreover, the indirect costs of cybercrime, such as reputational damage and loss of customer confidence, can have long-lasting effects on an organization's financial health (Ponemon Institute, 2019). When a company suffers a data breach, it often faces a decline in stock market valuation and a loss of market share as customers turn to competitors with perceived stronger security measures (Sullivan et al., 2018). This erosion of trust can be particularly damaging in sectors that rely heavily on customer confidence, such as banking, finance, and e-commerce. Additionally, the need for increased investment in cybersecurity measures, including advanced technologies, training, and incident response capabilities, further strains financial resources, diverting funds from other critical areas like innovation and growth (Clarke & Knake, 2010).

Cybercrime also exacerbates economic disparities and vulnerabilities across different regions and industries. Developing countries and small businesses often lack the resources and expertise needed to defend against sophisticated cyber threats, making them particularly vulnerable to economic disruption caused by cybercrime (Broadhurst, 2006). These entities may struggle to recover from a significant cyber attack, resulting in job losses, reduced economic activity, and a negative impact on the broader economy.

Furthermore, the interconnected nature of the global economy means that a cyber attack in one region can have cascading effects, disrupting supply chains and affecting markets worldwide (Rid & Buchanan, 2015). This interconnectedness underscores the need for a coordinated global response to cybercrime that enhances cybersecurity resilience across all sectors and regions.

In conclusion, the economic impact of cybercrime on global security is extensive and multifaceted, affecting not only direct financial losses but also broader economic stability and trust in digital systems.

The substantial costs associated with cybercrime highlight the importance of robust cybersecurity strategies and international cooperation to mitigate these risks. By understanding the economic dimensions of cybercrime, policymakers, businesses, and governments can develop more effective responses to protect the global economy and enhance resilience against evolving cyber threats.

3.2. Geopolitical Implications of Cybercrime

Cybercrime also has significant geopolitical implications, influencing international relations and national security. As cyberattacks become more sophisticated and state-sponsored, the line between cybercrime and cyberwarfare blurs, raising concerns about the use of cyberattacks as tools of geopolitical strategy (Clarke & Knake, 2010). State-sponsored cybercriminals often target critical infrastructure, government agencies, and private sector entities to gather intelligence, disrupt services, or undermine public trust in political institutions (Rid & Buchanan, 2015). These actions can lead to heightened tensions between nations, as states accused of perpetrating or sponsoring cyberattacks deny involvement and accuse others of similar activities, creating a cycle of suspicion and retaliation (Healey, 2011).

Furthermore, cybercrime has been used as a means of projecting power and influence in international relations. Nations may engage in cyber espionage to gain economic or military advantages, or use cyberattacks to influence political outcomes in other countries (Guitton, 2017). For example, the alleged Russian interference in the 2016 United States presidential election through cyber means has highlighted the potential for cybercrime to impact democratic processes and manipulate public opinion (Rid, 2020). Such actions undermine the integrity of political systems and contribute to a more volatile international environment, where digital operations can escalate into broader geopolitical conflicts (Valeriano et al., 2018).

The geopolitical implications of cybercrime also extend to the global governance of cyberspace. As cyber threats become more prominent, nations are increasingly focusing on developing international norms and agreements to regulate state behavior in cyberspace and enhance global cybersecurity (Lewis, 2018).

However, differing national interests, priorities, and perspectives on internet governance pose significant challenges to achieving consensus on these issues (Nye, 2014). Some countries advocate for a more open and free internet, while others prioritize sovereignty and control over digital spaces within their borders, leading to a fragmented approach to cybersecurity governance (Deibert, 2015).

In summary, the geopolitical implications of cybercrime are profound, affecting international relations, national security, and global governance. The use of cybercrime as a tool of statecraft, combined with the challenges of regulating cyberspace at the international level, underscores the need for collaborative efforts to develop norms, frameworks, and policies that enhance global security and stability. Understanding these geopolitical dimensions is essential for policymakers and security professionals seeking to address the complex and evolving nature of cyber threats.

Cybercrime has significant geopolitical implications, fundamentally altering the landscape of international relations and national security. The rise of state-sponsored cybercrime, where nation-states engage in cyber activities that blur the lines between criminal actions and acts of war, has led to increased tensions between countries (Rid & Buchanan, 2015). These activities often involve cyber espionage, sabotage, and the theft of sensitive data, targeting critical infrastructure and government institutions. For example, cyber attacks like the alleged Russian interference in the 2016 U.S. presidential election and the North Korean-linked WannaCry ransomware attack have highlighted how cybercrime can be used as a tool of statecraft to influence political processes and destabilize adversaries (Guitton, 2017). Such actions not only undermine trust between nations but also create an environment of suspicion and retaliatory behavior, complicating diplomatic relations and international cooperation.

The use of cybercrime as a strategic tool by states introduces a new dimension to global power dynamics. Unlike conventional warfare, cybercrime allows states to exert influence and achieve strategic objectives without the overt use of military force, making it an attractive option for asymmetric warfare (Valeriano et al., 2018). Cyber operations are often difficult to attribute definitively to a specific actor, providing plausible deniability for the perpetrators and complicating responses from the targeted states (Healey, 2011).

This ambiguity can lead to a lack of accountability and a cycle of escalation, where nations engage in tit-for-tat cyber operations that increase the risk of broader conflict (Rid, 2020). The potential for cybercrime to disrupt critical infrastructure, such as energy grids, financial systems, and communication networks, further underscores its strategic importance in modern geopolitical competition (Clarke & Knake, 2010).

In addition to its impact on state relations, cybercrime has significant implications for global governance and the regulation of cyberspace. The lack of international consensus on the rules and norms governing state behavior in cyberspace poses challenges for developing effective legal frameworks to combat cybercrime (Deibert, 2015). While initiatives like the Budapest Convention on Cybercrime and the United Nations' efforts to establish norms of responsible state behavior in cyberspace represent steps towards greater cooperation, differing national interests and perspectives on internet governance continue to hinder progress (Nye, 2014). Some countries advocate for a free and open internet, while others prioritize sovereignty and control over their digital spaces, leading to a fragmented approach to cybersecurity governance (Lewis, 2018).

In conclusion, the geopolitical implications of cybercrime are profound, influencing international relations, national security, and global governance. The strategic use of cybercrime by states, combined with the challenges of attribution and the lack of unified international regulations, highlights the complex and evolving nature of this threat. Addressing these challenges requires enhanced international cooperation, the development of clear norms and legal frameworks, and a commitment to building trust and accountability in cyberspace. By understanding the geopolitical dimensions of cybercrime, policymakers can better navigate the complexities of cyber diplomacy and work towards a more secure and stable global digital environment.

3.3. Technological Vulnerabilities and Cybersecurity Challenges

Technological vulnerabilities are at the heart of the cybercrime problem, presenting significant challenges for global security. Cybercriminals exploit weaknesses in software, hardware, and network configurations to gain unauthorized access to systems, steal data, and disrupt services (Sullivan et al., 2018).

As digital technologies become more complex and interconnected, the potential attack surface for cybercriminals expands, increasing the likelihood of successful cyberattacks (Brenner, 2010). For example, the proliferation of Internet of Things (IoT) devices, many of which lack robust security features, has created new opportunities for cybercriminals to infiltrate networks and launch attacks (Roman et al., 2013).

Moreover, technological advancements have enabled the development of more sophisticated cyberattack techniques, such as zero-day exploits, advanced persistent threats (APTs), and deepfake technologies (Lewis, 2018). These techniques allow cybercriminals to bypass traditional security measures, remain undetected for extended periods, and cause more significant damage (Clarke & Knake, 2010). For instance, APTs, which involve prolonged and targeted attacks on specific entities, are often used to steal sensitive information or sabotage critical infrastructure, posing severe risks to national security and public safety (Bodmer et al., 2012). The evolving nature of these threats requires constant adaptation and innovation in cybersecurity practices to stay ahead of malicious actors.

Additionally, the shortage of skilled cybersecurity professionals and resources further exacerbates the challenges of addressing technological vulnerabilities (Broadhurst, 2006). Many organizations, particularly small businesses and public sector entities, lack the expertise and financial capacity to implement comprehensive cybersecurity measures, making them attractive targets for cybercriminals (Sullivan et al., 2018). This skills gap not only limits the ability of organizations to protect themselves against cyber threats but also hampers efforts to respond effectively to incidents and recover from attacks (Krebs, 2012). Addressing this challenge requires significant investment in cybersecurity education, training, and capacity building at the national and international levels.

In conclusion, technological vulnerabilities and cybersecurity challenges are critical factors contributing to the impact of cybercrime on global security. The rapid pace of technological change, combined with the growing sophistication of cyber threats and the shortage of skilled professionals, underscores the need for a comprehensive and proactive approach to cybersecurity.

By addressing these technological dimensions, policymakers and security professionals can enhance global resilience against cybercrime and protect critical infrastructure and public safety.

3.4. Strategies for Enhancing Cybersecurity and Global Cooperation

Enhancing cybersecurity and fostering global cooperation are essential strategies for mitigating the impact of cybercrime on global security. One of the key strategies for enhancing cybersecurity is the development and implementation of robust cybersecurity frameworks and standards that provide guidelines for protecting critical infrastructure, information systems, and digital assets (Sullivan et al., 2018). These frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the ISO/IEC 27001 standard, offer a structured approach to managing cybersecurity risks, enabling organizations to identify, protect, detect, respond to, and recover from cyber incidents (NIST, 2018). By adopting these frameworks, organizations can improve their cybersecurity posture and resilience against cyber threats.

In addition to developing robust cybersecurity frameworks, international cooperation is crucial for addressing the global nature of cybercrime. Cybercrime often transcends national borders, making it difficult for individual countries to combat these threats alone (Broadhurst, 2006). International cooperation involves sharing information, intelligence, and best practices among nations, as well as collaborating on law enforcement efforts to investigate and prosecute cybercriminals (Lewis, 2018). Initiatives such as the Budapest Convention on Cybercrime and the European Union’s General Data Protection Regulation (GDPR) represent important steps toward enhancing international collaboration and establishing common standards for cybersecurity and data protection (Council of Europe, 2001; European Union, 2016).

Furthermore, public-private partnerships play a vital role in enhancing cybersecurity and promoting global cooperation. The private sector owns and operates a significant portion of the world’s critical infrastructure and is often at the forefront of technological innovation (Nye, 2014).

By collaborating with the private sector, governments can leverage the expertise, resources, and capabilities of businesses to enhance cybersecurity measures and develop more effective responses to cyber threats (Clarke & Knake, 2010). Public-private partnerships can also facilitate the exchange of threat intelligence, foster innovation in cybersecurity technologies, and support capacity-building efforts to strengthen global resilience against cybercrime (Valeriano et al., 2018).

Finally, fostering a culture of cybersecurity awareness and education is essential for enhancing global security. Cybersecurity is not solely the responsibility of governments and organizations; individuals also play a crucial role in protecting themselves and their communities from cyber threats (Brenner, 2010). By promoting cybersecurity awareness and education at all levels of society, from schools to workplaces, nations can empower individuals to recognize and respond to cyber threats effectively, reducing the overall risk of cybercrime (Ponemon Institute, 2019). Investing in cybersecurity education and training programs, as well as conducting public awareness campaigns, can help build a more resilient and secure digital environment for all.

4. Conclusion

The analysis of the impact of cybercrime on global security highlights the multifaceted nature of this evolving threat, emphasizing its significant economic, geopolitical, technological, and cooperative implications. Economically, cybercrime imposes substantial financial losses on individuals, businesses, and governments, while also eroding public trust in digital systems and the broader digital economy. The costs associated with cybercrime, including direct financial losses, reputational damage, and increased cybersecurity expenditures, demonstrate the critical need for robust cybersecurity measures to protect economic stability. Geopolitically, cybercrime blurs the line between criminal activity and state-sponsored actions, influencing international relations and posing severe risks to national security. The use of cybercrime as a tool of statecraft and the challenges of achieving consensus on global cybersecurity governance further complicate efforts to maintain international stability and peace.

Technologically, the rapid advancement of cyberattack techniques and the growing interconnectedness of digital systems exacerbate vulnerabilities, making it increasingly difficult to defend against sophisticated threats. The shortage of skilled cybersecurity professionals and resources amplifies these challenges, highlighting the urgent need for investment in cybersecurity education, training, and capacity building. To effectively combat cybercrime and enhance global security, it is essential to develop comprehensive cybersecurity frameworks, foster international cooperation, and promote public-private partnerships. Additionally, raising awareness and education on cybersecurity at all levels of society is crucial for building a more resilient and secure digital environment. By addressing these multifaceted aspects of cybercrime, policymakers, security professionals, and organizations can better protect global security and adapt to the ever-evolving cyber threat landscape.

5. References

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12

Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). Reverse deception: Organized cyber threat counter-exploitation. McGraw-Hill.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brenner, S. W. (2010). Cyberthreats: The emerging fault lines of the nation state. Oxford University Press.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management, 29(3), 408-433. https://doi.org/10.1108/13639510610684674

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. European Societies, 23(1), S47-S59. https://doi.org/10.1080/14616696.2020.1804973

Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. HarperCollins.

Cooper, H. (2010). Research synthesis and meta-analysis: A step-by-step approach (4th ed.). Sage Publications.

Council of Europe. (2001). Convention on Cybercrime. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Deibert, R. J. (2015). The geopolitics of cyberspace after Snowden. In D. Lyon (Ed.), Surveillance after Snowden (pp. 38-57). Polity Press.

European Union. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Flick, U. (2014). An introduction to qualitative research (5th ed.). Sage Publications.

Guitton, C. (2017). The waning of Western cyber deterrence. International Affairs, 93(6), 1317-1334. https://doi.org/10.1093/ia/iix207

Healey, J. (2011). A fierce domain: Conflict in cyberspace, 1986 to 2012. Cyber Conflict Studies Association.

Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge. https://doi.org/10.4324/9781315723555

Krebs, B. (2012). Spam nation: The inside story of organized cybercrime-from global epidemic to your front door. Sourcebooks.

Lewis, J. A. (2018). Economic impact of cybercrime—No slowing down. CSIS. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods, 16(1), 1-13. https://doi.org/10.1177/1609406917733847

Nye, J. S. (2014). The regime complex for managing global cyber activities. Global Commission on Internet Governance Paper Series, 1. https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

Ponemon Institute. (2019). 2019 Cost of a Data Breach Report. Retrieved from https://www.ibm.com/security/data-breach

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), 4-37. https://doi.org/10.1080/01402390.2014.977382

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sullivan, C., Clarke, R., & Larkin, C. (2018). The data breach triangle: Toward a framework for data breach prevention, detection, and response. Business Horizons, 61(6), 935-944. https://doi.org/10.1016/j.bushor.2018.06.004

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management, 14(3), 207-222. https://doi.org/10.1111/1467-8551.00375

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). Cyber strategy: The evolving character of power and coercion. Oxford University Press.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26(2), xiii-xxiii.