

## **Strategic Leadership Styles in the Digital Era: Lessons From Russia, the United States, and Israel for Indonesia's Cyber Defense Doctrine**

**Agung Widodo, Arif Harianto\*, Tarsisius Susilo, Andy Mustafa Akad,  
Joko Prasetyo**

Sekolah Staf dan Komando Tentara Nasional Indonesia

Email: 45agungwidodo@gmail.com arifharianto281@gmail.com\*

### **Abstract**

The development of information technology has presented new challenges in the defense sector, particularly in the cyber domain. Threats such as ransomware attacks, data leaks, and the potential for cyber warfare are not only technical but also strategic, as they can disrupt national stability and state sovereignty. Against this backdrop, the study examines strategic leadership in cyber defense by comparing the experiences of three countries: Russia, the United States, and Israel. The research aims to identify the strategic leadership patterns of cyber defense in these three countries, analyze their similarities and differences, and assess their relevance for Indonesia. The method employed is a qualitative approach, combining case studies and literature reviews to achieve a comprehensive understanding. The analysis reveals that Russia emphasizes centralized command and offensive capabilities, the United States prioritizes multi-sectoral collaboration, and Israel is distinguished by innovation and civil-military synergy. A common feature among the three is the framing of cyber strategic leadership as a national issue rather than merely a technical matter. For Indonesia, the findings underscore the need to develop an integrated national cyber defense doctrine based on national values and the involvement of all components of the nation. In conclusion, visionary, collaborative, and innovative strategic leadership will strengthen Indonesia's cyber defense, safeguard digital sovereignty, and contribute to achieving Golden Indonesia 2045. This study bridges leadership theory and defense doctrine by integrating conceptual and practical perspectives on cyber strategy, offering an interdisciplinary framework rarely addressed in Indonesian defense scholarship.

**Keywords:** Strategic Leadership, Cyber Defense, Indonesia.

## **INTRODUCTION**

In the midst of the geopolitical landscape of the 21st century, power between countries is no longer solely determined by conventional military capacity or economic advantage, but by dominance in the cyber and information domains. The sustainability of national sovereignty depends on how the state formulates strategies for managing digital space, including the ability to survive, attack, and influence public narratives. Leaders of major countries such as Russia, the United States, and Israel are not only pursuing advanced technologies, but are also building a strategic leadership style that bridges political decisions, defense doctrine, and the mobilization of digital resources (Defense, 2018; Tikk et al., 2010; Yin, 2018).

The use of *influence operations* in the cyber realm has become a new weapon in power competition. These countries are leveraging the ability of *cyber influence* to shape public perception, shake institutional trust, and intervene in democratic processes within hard-to-trace boundaries (House,

2018; Renz, 2018; Singer & Friedman, 2014). At the same time, countries that are known to be reluctant to face cyber challenges are beginning to formulate integrated cyber defense doctrines that combine prevention, active response, and the formation of digital resilience (Corporation, 2021; Intelligence, 2017; Nye, 2010; Sanger, 2012). The concept of cyber deterrence is now considered a new pillar in global defense doctrine due to the nature of cyber conflicts that are not always clearly defined, difficult to attribute, and have the potential to have far-reaching impacts on critical infrastructure ((CCDCOE), 2020; Lewis, 2017; Miles et al., 2019).

In the digital age, strategic leadership acts as a crucial link between political vision and the development of a cyber defense doctrine. Effective leadership in this realm requires not just technological foresight but also the strategic discernment to know when to be offensive or defensive, and the ability to craft national policies for the rapid mobilization of digital resources. Foundational theories such as Transformational, Adaptive, and Military Strategic Leadership provide a conceptual framework for this analysis, highlighting the need for vision, resilience, and strategic resource management. While traditionally studied in business or civil contexts, the application of these leadership styles to cyber defense strategy remains a significant research gap that this work aims to address (Indonesia, 2015; Informatics, 2020).

This research is particularly urgent for Indonesia, which faces complex cyber threats ranging from government system attacks to organized disinformation campaigns (Directorate, 2021; Giles, 2019; Inkster, 2016). The Indonesian National Armed Forces (TNI) currently lacks a fully integrated cyber military structure within its operational doctrine, with some proposals even suggesting the establishment of a dedicated Cyber Force. As a vast archipelagic nation, Indonesia's unique challenges include dispersed digital infrastructure, connectivity disparities, and vulnerability to information supply chain disruptions, demanding a leadership approach that can align national values like Pancasila with practical cybersecurity needs (N. R. Council, 2021; Creswell, 2018; Giles, 2016).

To design an ethical and adaptive Indonesian cyber defense doctrine relevant to its 2045 aspirations, this article will analyze the strategic leadership styles of Russia, the US, and Israel in managing their digital resources. By examining these cases through the lenses of transformational, adaptive, and military strategic leadership, it seeks to extract concrete lessons (Agency, 2022; Clarke & Knake, 2019; Zürich), 2019). The goal is to inform a doctrine that is not only effective in addressing modern multi-domain threats but also uniquely suited to Indonesia's national character and strategic context (A. Council et al., 2012).

This research is structured to answer three pivotal questions, focusing on the patterns of digital-cyber leadership styles in the defense strategies of Russia, the United States, and Israel. It further investigates the implicit impact

of these leadership models on their doctrinal structures, operational readiness, and institutional synergy. The ultimate aim is to determine how the values of Pancasila, the spirit of struggle, and the national defense philosophy can be integrated into Indonesia's own cyber defense doctrine, drawing concrete lessons from these international case studies.

The significance of this study is both academic and practical, as it seeks to bridge the separate research domains of leadership theory and digital defense strategy. By providing a comparative analysis of global leadership patterns, the findings are expected to offer crucial conceptual input for Indonesian defense policymakers and TNI decision-makers. This will aid in developing a credible, character-driven, and efficient cyber doctrine to effectively confront the complex challenges of the digital era and support the nation's progress toward Golden Indonesia 2045.

In the rapidly evolving landscape of global security, the digital domain has emerged as a critical arena of national power, demanding leadership that transcends conventional military strategy. While extensive scholarly work exists on strategic leadership within business and civil contexts, a significant research gap remains concerning its specific application and impact on the formulation and execution of national cyber defense doctrines. This study addresses this void by interrogating the distinct patterns of strategic leadership employed in the cyber realms of Russia, the United States, and Israel, moving beyond a purely technical analysis to explore how leadership styles fundamentally shape doctrinal structures, operational readiness, and institutional synergy. The novelty of this research lies in its interdisciplinary framework, which bridges leadership theory—drawing on transformational, adaptive, and military strategic models—with the practical imperatives of digital defense, an intersection rarely explored within the context of Indonesian defense scholarship.

The primary purpose of this research is to systematically analyze the strategic leadership styles in cyber defense of Russia, the US, and Israel to extract concrete, contextualized lessons for Indonesia. It seeks to determine how the values of Pancasila, the national defense philosophy, and the spirit of struggle can be integrated into a uniquely Indonesian cyber defense doctrine. The ultimate benefit of this study is twofold: academically, it enriches literature by fusing leadership theory with cybersecurity strategy, offering a novel comparative lens. Practically, it provides a foundational conceptual and strategic input for Indonesian defense policymakers and the Indonesian National Armed Forces (TNI), aiding in the development of a character-driven, efficient, and sovereign cyber doctrine to secure Indonesia's digital future and support the nation's progress toward the Golden Indonesia 2045 vision.

## RESEARCH METHOD

This research employed a qualitative approach to examine in depth the patterns of *strategic leadership* in the cyber and information domains, and their

relevance to Indonesia's defense needs. The study prioritized analytical depth over data breadth.

The research design was a comparative case study focusing on Russia, the United States, and Israel, selected for their differing *strategic leadership* characteristics and shared emphasis on managing digital and cyber resources. Russia was selected due to Vladimir Putin's leadership focus on information operations and cyber influence as geopolitical instruments. The United States was included for its strong presidential tradition in shaping both offensive and defensive cyber doctrines. Israel was chosen for successfully integrating technological, military, and intelligence capabilities to overcome resource limitations through digital innovation.

Data were sourced from academic literature, policy documents, credible international media, and Indonesian national defense references. Key policy sources included the United States National Security Strategy, Russia's Doctrine of Information Security, and Israel's cyber defense policy. Indonesian sources included the Defense White Paper, the National Long-Term Development Plan (RPJPN), and Ministry of Defense/TNI documents related to cyber strategy. Literature was obtained via academic databases, think tank reports, and official government publications.

Data analysis applied content analysis with a thematic approach, proceeding through data reduction, thematic categorization, interpretation based on established leadership theories, cross-country comparison within Indonesia's defense value framework, and synthesis of recommendations for Indonesia's cyber defense doctrine.

Research validity was ensured through source triangulation, combining academic literature, official policy documents, and reports from international research institutions. The application of established leadership theories strengthened the conceptual framework, while comparative analysis ensured the findings were actionable and relevant to both academic discourse and practical policy development.

## RESULTS AND DISCUSSION

### Russia's Strategic Leadership in Cyber Defense

Russia views cyberspace as the fifth strategic domain after land, sea, air, and space. This is reflected in the *Military Doctrine of the Russian Federation* of 2010 and updated in 2014 and 2020, which emphasizes that threats in the field of information and cyber are no less dangerous than conventional military threats. Since the era of Vladimir Putin's leadership, cyberspace has been seen not only as a technological arena, but also as a geopolitical and ideological instrument that can be used to defend sovereignty and expand Russia's global influence.

Russia's leadership in this context is authoritarian, centralized, and strategic-military in character. All state instruments, especially the *Federal Security Service (FSB)*, the *Main Directorate of the General Staff (GRU)*, and

the Ministry of Defense, are used in a coordinated manner to build superiority in cyberspace. In contrast to the democratic model that emphasizes transparency, Russia adopts a closed and hierarchical approach, in which the President becomes a central actor in strategic decision-making. This reflects an autocratic-strategic leadership style, which emphasizes full control of the center of power over all aspects of digital security.

The main characteristic of Russia's leadership in the digital realm is its orientation to offensive cyber warfare. Some of the prominent cases include:

- A cyberattack on Estonia (2007) that paralyzed the national banking, media, and communication infrastructure for weeks.
- The attack on Georgia (2008), which was carried out in conjunction with conventional military operations, marked the integration of cyberspace with combat operations on the ground.
- Intervention in the United States Election (2016), in which Russia was accused of using cyber operations and disinformation campaigns to influence public opinion and political outcomes.

These examples show that Russia is using cyberspace as a foreign policy instrument to expand influence, weaken enemies, and challenge Western dominance. In the perspective of leadership theory, this pattern reflects strategic-military leadership, in which political, military, and technological forces combine to achieve long-term strategic goals.

For Indonesia, the Russian leadership model provides two important lessons. First, the need for the integration of political and military leadership in handling cyber threats. With a clear command mechanism, threats can be responded to quickly and in a coordinated manner, creating a *deterrence effect*. Second, Russia shows the urgency of strategic investment in cyber technology as part of force *development*. However, the authoritarian and closed aspects of Russian leadership have the potential to be incompatible with Indonesia's democratic political system and based on Pancasila. Therefore, a more relevant lesson is on the aspect of the seriousness of strategic investment, centralized command, and the integration of instruments of national power, not on repressive patterns that are contrary to democratic values and human rights.

#### United States Strategic Leadership in Cyber Defense

The United States (US) is the first country to officially place cyberspace as the domain of military operations equivalent to land, sea, air, and space. Since the establishment of the U.S. Cyber Command (USCYBERCOM) in 2009, the U.S. government has emphasized that control of cyberspace is an integral part of its global leadership. The *National Cyber Strategy* (2018) and *Department of Defense Cyber Strategy* (2018) documents emphasize the great vision of the US to achieve cyberspace superiority, namely the ability to control cyberspace in order to maintain its national interests and hegemony at the global level.

U.S. strategic leadership in the cyber field can be categorized as institutional and collaborative. The President as Commander-in-Chief of the

Armed Forces sets the general policy direction, while USCYBERCOM, the National Security Agency (NSA), the Department of Homeland Security (DHS), and other intelligence sectors carry out technical and operational functions. This leadership system shows a pattern of shared leadership, where authority is not centralized on a single figure, but is divided institutionally to ensure effectiveness and accountability.

The main feature of US leadership in the digital era is the application of transformational leadership principles. Referring to the theories of James MacGregor Burns and Bernard Bass, transformational leadership emphasizes big vision, collective motivation, and continuous innovation. In the cyber context, the U.S. is building a long-term vision to maintain superiority through several key strategies:

a. **Technological Innovation.**

The U.S. encourages research and development in artificial intelligence (AI), quantum computing, big data, and cloud security as the basis of cyber defense. Leadership in this innovation is not only driven by the government, but also by large technology companies such as Microsoft, Google, Amazon, IBM, and Palantir that are part of the national defense ecosystem.

b. **Global Alliance.**

The US leverages multilateral organizations such as **NATO**, the Quad (US, Japan, India, Australia), and bilateral cooperation with European and Asian countries to strengthen global cybersecurity networks. NATO, for example, established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, with strong support from the US. This leadership shows that cyberspace is seen as a collective arena, where the power of alliances becomes hegemonic instruments.

c. **Public-Private Synergy.**

Unlike Russia, which tends to rely on the state as a single actor, the U.S. is building a collaborative cyber defense ecosystem. Private companies are given a big role in protecting the national digital infrastructure, ranging from the banking system, electricity grid, to strategic communications. This collaboration underscores the hallmarks of U.S. leadership that is adaptive, democratic, and based on a *whole of nation approach*.

For Indonesia, the U.S. leadership model provides important inspiration. First, cyber leadership must be placed within a national policy framework involving various ministries and institutions, not just the military. Second, it is necessary to build public-private synergy in protecting national critical infrastructure, considering that most of Indonesia's data and digital systems are managed by private companies. Third, Indonesia needs to actively build international cooperation in regional and global forums, as part of cyber defense diplomacy.

However, there are also aspects that need to be watched out. U.S. digital leadership often gives rise to the impression of technological

hegemony, where global security, software, and digital infrastructure standards are heavily influenced by the interests of Washington and U.S. tech giants. This requires Indonesia to maintain digital sovereignty by strengthening national regulations and building domestic technological capacity.

### **Israel's Strategic Leadership in Cyber Defense**

Israel is known as one of the countries with the most prominent strategic leadership in the field of cyber defense. Historical factors in the form of conflict-ridden geopolitical conditions made Israel develop a defense strategy based on technological innovation from an early age. One of the manifestations is the establishment of the Israel National Cyber Directorate (INCD) which is directly under the Prime Minister, thus ensuring full integration between political policy, national security, and technological development. The strategic position of the INCD reflects that Israel views cyberspace not only as a technical domain, but as a strategic battlefield that determines the survival of the country.

Israeli leadership is network-centric leadership, which is a leadership style that emphasizes synergy between state actors (government and military) and non-state actors (technology industry, academia, and start-ups). This model enables the creation of a resilient, adaptive, and innovative cyber defense ecosystem. Israel is known as a "Start-up Nation", with more than 6,000 tech startups that are heavily engaged in cybersecurity. The government's strong support through pro-innovation policies, research investments, and collaboration between Unit 8200 (the Israeli military's cyber intelligence unit) and the civilian sector makes Israel's strategic leadership highly dynamic and innovation-based.

One of the important milestones that demonstrates Israel's leadership excellence in cyber defense is Operation Stuxnet (2010), which is believed to have been carried out with the United States to destroy Iran's nuclear facility at Natanz. This attack shows that Israel has not only mastered defensive capabilities, but also offensive cyber operations with high precision. This success affirms Israel's position as a pioneer in utilizing cyber technology as a political, military, and diplomatic tool. In addition, Israel's strategic leadership in the digital realm also emphasizes the development of human capital. The recruitment of talented young talent into military cyber units from an early age, such as through the recruitment program at Unit 8200, creates a continuous cycle of innovation. Many alumni of the unit then built cybersecurity start-ups that support both the public and private sectors. Thus, Israel has succeeded in connecting political, military, and civilian leadership in one mutually reinforcing cyber ecosystem.

For Indonesia, the Israeli model provides several important lessons. First, the importance of institutional integration of cyber defense at the national level, so that coordination is not fragmented between government, military, and private sector agencies. Second, the development of a national digital

innovation ecosystem must be spurred by the support of visionary leadership, daring to take risks, and providing space for the creativity of the younger generation. Third, although Indonesia does not need to imitate Israel's offensive approach that has the potential to cause geopolitical escalation, the spirit to develop defensive cyber capabilities based on superior human resources should be made a strategic priority.

### **Comparative Analysis of Russia – United States – Israel**

The three countries—Russia, the United States, and Israel—represent different models of strategic leadership in cyber defense, but both place cyberspace as a national strategic domain. A fundamental commonality that can be identified is that they all consider cyber not just a technical or digital security issue, but as an instrument of national power that has geopolitical, economic, and military implications. Thus, leadership in this domain is positioned on a par with leadership in the conventional military realm.

However, there are fundamental differences in each country's leadership style.

a. **Russia Put Centralization and offensive power.** Russian leadership under Vladimir Putin emphasizes Authoritarianism in decision-making, where all state instruments—military, intelligence, and non-state actors that are controlled, are mobilized to strengthen cyber capabilities. Doctrine *Informatsionnaya voyna* (information war) shows that Russia is using cyberspace as a foreign policy tool, both to weaken opponents and expand geopolitical influence.

b. **United States Developing a model Collaborative and Hegemonic Leadership.** With the formation U.S. Cyber Command (USCYBERCOM) and strategy *Cyberspace Superiority*, the U.S. emphasizes collaboration between governments, the military, the private sector, academia, as well as international alliances such as NATO and the Quad. This pattern shows the approach transformational leadership, where the vision of digital leadership is geared towards maintaining global dominance through technological innovation and multilateral diplomacy.

c. **Israel Displaying models Innovative leadership with civil-military synergy.** In contrast to authoritative Russia or the hegemonic US, Israel places more emphasis on creation National Innovation Ecosystem, by integrating start-ups, technology industries, and cyber military units (such as Unit 8200). In this way, Israel has succeeded in creating an adaptive and creativity-based leadership, while strengthening its cyber defense capabilities through superior human resources.

From this comparison, it can be seen that Russia, the US, and Israel both consider cyber as a national strategic issue, but the differences in leadership styles provide a unique pattern:

- a. Russia relies on Coercive forces and political centralization;
- b. The US emphasizes Cross-sector collaboration and global hegemony;
- c. Israel highlights innovation and civil-military integration.

For Indonesia, an important lesson from this comparison is the need to find a cyber leadership model that is in accordance with the character of national democracy. Russia's authoritarian approach is difficult to apply in the Indonesian context, while the collaborative U.S. model and the innovative Israel are more relevant to building a strong and sustainable national cyber defense ecosystem.

### **Relevance for Indonesia: The Urgency of the National Cyber Defense Doctrine**

Indonesia is currently facing serious challenges in the increasingly complex and diverse cyber domain. Data from the State Cyber and Cryptography Agency (BSSN) shows that throughout 2022 alone, there were more than 11.8 million cyber traffic anomalies, including ransomware attacks, personal data leaks, and disinformation that has the potential to divide the nation's unity. The threat is not only technical, but also strategic because it targets vital national infrastructure such as energy, transportation, communications, and finance. In a global geopolitical context marked by great power rivalries, the potential for cyber warfare against Indonesia cannot be ignored, especially given Indonesia's strategic position in the Indo-Pacific.

Until now, although Indonesia has had the State Cyber and Cryptography Agency (BSSN) as the main institution that coordinates cybersecurity, the national cyber defense doctrine has not been fully integrated into the country's defense system. This is in contrast to major countries such as Russia, the United States, and Israel, which clearly place the cyber domain in their national defense doctrines. This shows the urgency for Indonesia to immediately formulate a comprehensive, integrated, and visionary cyber defense doctrine.

From the comparative analysis of three countries (Russia, the US, Israel), there are a number of important lessons that are relevant for Indonesia:

- a. From Russia, Indonesia can learn about the importance of Centralization of command and cyber placement as Strategic priorities in national defense. Russia shows that consolidated cyber power under the supreme political leadership can increase effectiveness Deterrence.
- b. From the United States, its relevance lies in the model Cross-sector collaboration. Indonesia needs to encourage synergy between the government, the TNI, academics, the technology industry, and civil society in building a cybersecurity ecosystem. This kind of collaboration is in line with the democratic principles of Pancasila and the spirit of mutual cooperation that is the nation's identity.
- c. From Israel, Indonesia learned a lesson about The Urgency of Developing a Digital Innovation Ecosystem and Superior Human Resources. Israel proves that young talents and tech start-ups can be strategic assets in cyber defense. For Indonesia, this is important to support national digital transformation and answer the need to face cyber threats based on cutting-edge technology.

Based on these lessons, Indonesia's strategic leadership in the digital era must be able to formulate a national cyber defense doctrine with the following characteristics:

- a. Based on national values: Indonesia's cyber defense doctrine must be rooted in Pancasila, the 1945 Constitution, and the motto *Bhinneka Tunggal Ika* to be in harmony with national identity and strengthen political and moral legitimacy.
- b. Integrating all components of the nation: Cyber defense is not only the responsibility of the main components (TNI and BSSN), but must also involve the backup component (academics, professionals, technology community) and supporting components (private industry, civil society).
- c. Oriented towards digital sovereignty: Personal data protection, critical infrastructure security, and the prevention of foreign interference in the digital space must be top priorities, while supporting the vision *Indonesia Gold 2045*.

With visionary, collaborative, and rooted in national values, Indonesia can build a resilient digital resilience. This is not only to anticipate asymmetric threats in the cyber age, but also to strengthen national stability and national competitiveness in the long term.

## CONCLUSION

The comparative analysis of Russia, the United States, and Israel demonstrates that strategic leadership is a decisive factor in shaping cyber defense doctrines, with each nation exemplifying distinct models—authoritarian-centralized, collaborative-hegemonic, and innovative network-centric—while uniformly treating cyberspace as a strategic domain vital to sovereignty and geopolitical influence. For Indonesia, the core lesson is the necessity of a visionary and proactive national cyber defense doctrine, firmly grounded in national values, integrating strong command cohesion, multi-sectoral collaboration, and sustained digital innovation to achieve *Golden Indonesia 2045*. To advance this understanding, future research could adopt quantitative or mixed-methods approaches to measure correlations between leadership traits and cyber defense effectiveness, broaden the comparative scope to include key Indo-Pacific actors such as China, India, and Singapore, and examine micro-level institutional, regulatory, and cultural barriers to implementing an integrated doctrine, thereby bridging strategic concepts with actionable policy and operational structures.

## REFERENCES

- Agency, N. C. and C. (2022). *Annual report on national cybersecurity monitoring 2022*. BSSN.
- (CCDCOE), N. C. C. D. C. of E. (2020). *About us*. CCDCOE.
- Clarke, R. A., & Knake, R. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin.

- Corporation, R. (2021). *Strategic competition in cyberspace*. RAND Corporation.
- Council, A., Kramer, F. D., Butler, R. J., & Lotrionte, C. (2012). *Cybersecurity: Changing nature of U.S. national security and defense*. Atlantic Council.
- Council, N. R. (2021). *A strategic study of Indonesia's cyber defense*. Wantannas RI.
- Creswell, J. W. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- Defense, U. S. D. of. (2018). *Department of Defense cyber strategy*. DoD.
- Directorate, I. N. C. (2021). *The INCD's mission and role*. Government of Israel.
- Giles, K. (2016). *Russia's "new" tools for confronting the West: Continuity and innovation in Moscow's exercise of power*. Chatham House.
- Giles, K. (2019). *Moscow rules: What drives Russia to confront the West*. Chatham House.
- House, T. W. (2018). *National cyber strategy of the United States of America*. The White House.
- Indonesia, M. of D. of the R. of. (2015). *Indonesian Defense White Paper*. Ministry of Defense of the Republic of Indonesia.
- Informatics, M. of C. and. (2020). *Digital Indonesia Roadmap 2021–2024*. Kominfo.
- Inkster, N. (2016). *Information warfare and the future of cyber conflict*. Routledge.
- Intelligence, O. of the D. of N. (2017). *Assessing Russian activities and intentions in recent US elections*. ODNI.
- Lewis, J. A. (2017). *Public-private partnerships in cybersecurity*. Center for Strategic and International Studies.
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2019). *Qualitative data analysis: A methods sourcebook* (4th ed.). SAGE Publications.
- Nye, J. S. (2010). *Cyber power*. Harvard Kennedy School, Belfer Center for Science and International Affairs.
- Renz, B. (2018). *Russia's military revival*. Polity Press.
- Sanger, D. E. (2012). *Confront and conceal: Obama's secret wars and surprising use of American power*. Crown Publishers.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
- Tikk, E., Kaska, K., & Vihul, L. (2010). *International cyber incidents: Legal considerations*. Cooperative Cyber Defence Centre of Excellence.
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.
- Zürich, C. for S. S. (CSS E. T. H. (2019). *Cyber influence operations: A national security threat*. CSS ETH.