Journal of Science, Innovation and Creativity
Vol. 5 No. 1 (2026): ISSN (Online): 2958-454X
DOI: https://doi.org/10.58721/jsic.v5i1.1671
The Unintended Consequences of Cyber Warfare: A Case Study of the Iran–Israel Conflict

The Unintended Consequences of Cyber Warfare: A Case Study of the Iran-Israel Conflict

Philemon Sengati
University of Dodoma, Tanzania

Article History
Received: 2025-09-02
Revised: 2026-04-02
Accepted: 2026-04-09
Published: 2026-04-13

Keywords
Conflict
Cybersecurity
Statecraft
War

How to cite:
Sengati, P. (2026). The Unintended Consequences of Cyber Warfare: A Case Study of the Iran-Israel Conflict. *Journal Science, Innovation and Creativity, 5*(1), 39-48.

Abstract
Cyber warfare is one aspect of statecraft that has grown to be more significant over time due to its covert nature and affordability in terms of achieving certain strategic goals. This study seeks to investigate the unintended consequences of cyber warfare, considering the Iran-Israel conflict situation. The paper endeavours to explore the unintended outcomes of cyber warfare on the targets of both nations as well as the possible implications of such cyber operations in the security and governance realm. This research will adopt a qualitative case study design where the researcher will conduct a secondary systematic literature review of articles from scholarly sources. Thematic analysis of the reviewed secondary data will reveal some of the key unintended impacts associated with cyber operations. From the findings, it is evident that the use of cyber warfare in Iran-Israel has led to some key side effects including, the impact of cyber warfare on civilian infrastructure, economic consequences of cyber warfare, escalation in cyber warfare, extension of cyber capabilities to non-state actors, and making it difficult to distinguish between war and peace. The paper concludes that despite its reputation for accuracy, cyber warfare can be quite unpredictable, with the possibility of having wider implications than what can be expected in terms of achieving strategic objectives by the states. The paper calls for the formulation of international norms and regulations, investment in cybersecurity, and cooperation among the states in order to minimise the dangers of cyberwarfare. Lastly, the paper draws attention to the paradoxical nature of cyberwarfare, which is intended to serve as an instrument of control but ends up being uncontrollable.

Introduction

Cyber war is a more visible tool of statecraft, which provides strategic benefits by being covert, deniable, and low-cost. This paper investigates the unintended result of cyber warfare using a case study of the Iran-Israel war. The fast development of digital technologies has radically altered the nature of modern conflict and made cyber warfare one of the main tools of state power. However, unlike traditional warfare, cyber operations are not always visible; they can be deniable and covert, creating profound strategic impacts without physical engagement. Consequently, cyberspace has become an important sphere of contention with land, sea, air and space. Researchers in International Relations and Cybersecurity Studies tend to believe that cyber capabilities allow states to achieve both political and military goals without bearing the direct costs and risks of conventional warfare (Libicki, 2009; Nye, 2017; Lindsay, 2020). The long-term rivalry between Iran and Israel is one of the brightest examples of a long-term cyber conflict. A long-standing geopolitical, ideological, and security-related

confrontation has steadily moved into the digital sphere, where both nations use cyber technologies to spy on, disrupt, and send strategic signals. Cyber operations have become part of their overall shadow war, supplemented by conventional and proxy-based engagements over the past decade (Valeriano & Maness, 2015; Tabatabai, 2020).

Such a development is part of a larger international trend in which cyber capabilities are becoming increasingly integrated into national security policy. The high point of the militarisation of cyberspace was the Stuxnet attack in 2010, which is widely regarded as the first cyberattack to cause physical damage to critical infrastructure (Lindsay, 2013; Zetter, 2014). Undoubtedly, it was a successful venture as the cyber tool was able to disrupt the nuclear programme of Iran as well as destroy its uranium enrichment facility, making evident the possibility of cyber means to have an impact equivalent to that of the kinetic one. Nonetheless, it was another milestone in the development of cyber warfare as it marked the emergence of a precedent of the offensive cyber-attacks and led to the proliferation of cyber weapons, particularly in Iran. Therefore, it should be noted that there is a dual nature of cyber warfare as it offers possibilities, at the same time posing threats to states.

There are many operations in the Iran-Israel rivalry regarding cyber means. These may include cyber espionage, sabotage of the critical infrastructure, and the implementation of information operations. All these operations can be conducted at a time when there is no declaration of war by the involved sides, which results in a situation of permanent low-intensity warfare. It is suggested that the grey zone interactions of this kind become common nowadays as states seek to achieve strategic goals with minimal escalations of military actions (Mazarr et al., 2015; Smeets, 2022). However, the implications associated with the operations have been the subject of many concerns because of their cumulative effects. While the existing literature about cyber warfare has been growing, the literature is mainly concerned with the strategic uses of the weapon. Despite the informativeness of such views, they do not address the unintended consequences associated with the operations. As it has been noted, the attacks have been having an adverse effect on more than just the target countries. Indeed, the nature of digital communication allows the disturbances to have effects that go beyond the objectives of the attackers (Buchanan, 2020; Healey, 2022).

The result is the emergence of both unintended and counterproductive consequences in relation to the strategic interests of the warring sides. Therefore, this research work addresses the identified gap in the current body of knowledge by analysing the unintended consequences of cyber warfare through a thorough case study of the Iran-Israel conflict. The paper utilises some lessons learned from security studies and the interdisciplinary approach to conflicts in cyberspace in order to focus its analysis not on strategic results of the cyber operations but rather on their broader implications, which are often ignored by research. The implications of the use of the cyber capabilities will be analysed across several domains such as civil infrastructure, economic networks, dynamics of escalation and spread of cyber technologies. The main hypothesis advanced in this paper is that cyber war, despite its apparently predictable and controlled character, is a highly uncertain activity, resulting in a series of complex system-level effects. In order to prove the proposed hypothesis, theories of deterrence, complexity and unintended consequences will be employed to demonstrate that any use of cyber capabilities is associated with emergence of second and third-level effects, which redefine the very nature of conflicts.

In addition to the above, the study also contributes to the ongoing discourse about the metamorphosis of conflicts in the digital age. According to the research, the impact of cyber warfare leads to the blurring of boundaries between war and peace, combatants and civilians, and states and non-state entities. Such ambiguity has severe implications for governance, accountability, and the protection of critical infrastructure. As cyber capabilities continue to evolve and proliferate, the importance of

understanding their inadvertent impacts has become crucial for policymakers and practitioners alike. In conclusion, the example of Iran and Israel is a valuable framework for examining the wider implications of cyber warfare. The current paper offers a more nuanced interpretation of cyber conflicts as an intricate and dynamic process by examining the idea of unintended consequences.

Literature Review

The emergence of cyber warfare as an important topic of study in global security studies has attracted considerable scholarly attention in the fields of International Relations, security studies, and cybersecurity studies. Prior literature conceptualised cyber warfare as a form of espionage and disruption first and foremost (Libicki, 2009), while modern literature has focused on cyber warfare's role in shaping strategic competition at below-war levels (Valeriano, Jensen, and Maness, 2018; Kello, 2017). In the current discourse, cyber activities have been viewed as components of grey zone conflicts, which ensure continued interaction despite the lack of any war-like activity (Mazarr et al., 2015; Lindsay, 2020).

Contemporary literature (2020-2025) has shifted its focus towards exploring the long-term impact of cyber activities rather than their strategic implications. According to Buchanan (2020) and Healey (2022), cyber warfare entails system-level risks since digital infrastructures are interdependent. Similarly, another body of literature, such as Slayton (2021) and Smeets (2022), highlights the limitations of cyber operations and asserts that their effects are difficult to control. It can lead to unintended repercussions for different industries and jurisdictions. The research works refute the prior notion of the precision and locality of cyber tools.

The struggle for supremacy between Israel and Iran has recently attracted the attention of academic writings on cyber conflicts. After the Stuxnet attack, the Israel-Iran struggle has gained significance among academics due to its role in cyberspace warfare (Zetter, 2014; Lindsay, 2013). Current works (Tabatabai, 2020; Byman, 2023) argue that the cyber aspects of the rivalry have led to a discontinuous and complicated cyber war involving both states and non-state actors.

There is also an emerging trend focusing on the socio-economic consequences of cyber war. Recent studies since 2021 suggest that civilian infrastructures, like the health, finance, and logistics sectors, have become more vulnerable (Carr, 2021; ENISA, 2023). Moreover, other researchers, such as Nye (2022) and Rid (2023), underscore the role of cyber operations in shaping information environments, including disinformation and civilian psychologies.

While these developments have taken place, one glaring weakness remains. Much of the existing scholarship addresses unintended consequences, such as civilian deaths, escalation dynamics, and technology diffusion, as tangential topics instead of central research objects. Furthermore, there are few attempts to link these effects together in one empirical exercise. This paper seeks to remedy this deficiency by emphasising unintended consequences as the core problem under investigation and by examining the longitudinal evolution of the cyber conflict between Iran and Israel.

Theoretical Framework

In this research paper, the theoretical framework that has been adopted is a multi-theoretical approach, which integrates deterrence theory, complexity theory, and the theory of unintended consequences in the International Relations field.

The strategic rationale for cyber-attacks is grounded in deterrence theory. Deterrence involves the threat of reprisal to dissuade the adversary from acting (Schelling, 1966). Nonetheless, in cyberspace, the deterrence process is undermined by the problems of attribution, anonymity, and low-cost of operation (Nye, 2017; Smeets, 2022). In contemporary literature, it is argued that cyber deterrence is

partial and unsustainable, leading to sustained low-intensity warfare instead of strategic stability (Lindsay, 2020). In the particular scenario of Iran-Israel relations, there is no use of cyber operations as a deterrence measure. Cyber operations are rather used as a signalling, coercive, and limited retaliatory measure.

In addition to providing an understanding of cyber warfare as being unpredictable and non-linear in character, complexity theory can help in explaining how the attacks spill-over into other areas due to the interconnectedness of digital devices (Mitchell, 2009; Buchanan, 2020). Contemporary scholarship argues that it is becoming increasingly clear that the impact of cyber operations can exceed the target system and affect a much wider range of socio-technological systems (Healey, 2022). In this regard, the relevance of this theory becomes evident in the discussion of the spill-over effects associated with cyber-attacks in the Iran-Israel case.

The key analytical approach to be employed in this research is the theory of unintended consequences, originally developed by Merton (1936). According to this theory, intentional actions frequently have an unintended effect, which could even differ completely from the expected outcome. The application of this theoretical concept in the field of security in modern times draws attention to the importance of technologies as the element which changes the essence of war and its second- and third-order effects (Slayton, 2021; Rid, 2023). In this case, it refers to the spiral of escalation, proliferation, and increased vulnerability of non-targeted systems during cyber warfare.

The integration of all these theories provides a complete paradigm of research on cyber warfare. The use of deterrence theory will help in knowing why such cyber-attacks are employed, the application of complexity theory will assist in understanding the unpredictability of their outcomes, and the theory of unintended consequences will help in understanding why there is a gap between expected and actual results. Taken together, these constructs provide an excellent foundation of knowledge regarding the evolution of the Iran-Israel cyber warfare and its significance to world security.

Methodology

Research Design

This paper employs a qualitative case study design to examine the unintended effects of cyber warfare in the rivalry between Iran and Israel. The case study approach is especially appropriate for analysing dynamic and complex phenomena in real-world environments, as well as for situations where the boundaries between the phenomenon and its context are unclear (Yin, 2018). It is a single-case explanatory design that uses the Iran-Israel cyber conflict as a critical, information-rich case. The case is universally acclaimed as a paradigm shift in modern cyber warfare, especially since the Stuxnet operation signalled a new beginning in the militarisation of cyberspace. The design also allows for a longitudinal examination of events from the beginning of the 2010s to current escalations, enabling tracking over time.

Although the single-case design will enable analysis that is rich in context and in-depth, it has some limitations. In particular, the results might not generalise to other contexts of cyber conflict due to the geopolitical and strategic peculiarities of the Iranian-Israeli conflict. Also, this use of qualitative interpretation creates the risk of researcher subjectivity, which is countered by systematic processes and triangulation.

Data Sources and Collection

Secondary sources were the only data sources available for this study due to the sensitive and confidential nature of cyber operations. A systematic literature review was conducted, utilising scholarly literature, policy and institutional reports, and authoritative media sources. Peer-reviewed

journal articles and academic books about cyber warfare, international relations, and security studies were used as academic sources. Respected organisations, such as international security think tanks and cybersecurity agencies, were used to obtain policy and institutional reports. Moreover, confirmed media reports were included to document specific cyber-attacks and their consequences.

A systematic search strategy was used to review the documents systematically. Scholarly search engines and databases, such as Google Scholar, Scopus, Web of Science, and institutional repositories, were used to retrieve data. Other sources were obtained from official organisation websites, such as cybersecurity organisations and international policy think tanks. Key terms used in the search were cyber warfare, cyber conflict between Iran and Israel, Stuxnet, cyber escalation, cyber spill-over effects and unintended consequences of cyber operations. Searches were refined using the operators (AND, OR) to make searches relevant.

The sources used were chosen based on their relevance to cyber warfare or the Iran-Israel conflict, their publication dates (2010-2026), publisher credibility, and the availability of verifiable evidence. Sources with unidentified authorship, those containing unproven assertions, or those presenting redundant information that would not add analytical value were filtered out to preserve analytical rigour. The search and selection will take place over the six months between January 2025 and June 2025, enabling the extensive identification, screening, and review of pertinent materials.

Data Analysis

Thematic analysis is used as an analytic tool to examine patterns in collected data (Braun & Clarke, 2006). The analysis consisted of three main steps. Firstly, the process began with data familiarisation, in which the data was reviewed and organised to reveal patterns or themes. Secondly, the data was coded into categories based on identified themes, including the unintended consequences of cyber warfare, such as civilian infrastructure damage, economic impacts, escalation of conflict, and the development of cyber weapons. Thirdly, these identified themes were analysed and interpreted in light of the theoretical framework to determine why and how such unintended consequences arise.

Trustworthiness of the Study

To enhance the study's credibility, qualitative standards of trustworthiness were utilised. First, the data was triangulated to enhance its credibility by using several sources to verify the results. Next, dependability was ensured by providing consistent data collection and analysis processes. The confirmability of the data used in the study was ensured by relying on verifiable sources. Finally, transferability is achieved through a thorough analysis of the context of the Iran-Israel cyber conflict, which allows the generalisation of the findings to other cases of cyber warfare. Although the study is based on secondary data, which entails certain limitations, including the possibility of biased reporting and limited access to confidential information, it is inevitable when analysing cyber warfare issues.

Ethical Considerations

Ethics clearance is not required for this study, as no data will be collected from human subjects. Ethics have been maintained through accurate reporting of sources and non-use of any unverified and sensitive information.

Methodological Justification

In summary, the methodology discussed above facilitates an analytical investigation of the unintended effects of cyber warfare through a contextual framework that applies to both the specific instance of the Israel-Iran conflict and the broader phenomenon of digital warfare.

Results and Discussion

This part contains the results of the empirical study derived from the systematic review of documents. The present study is a qualitative empirical study because its data sources are qualitative secondary data. Results refer to consistent empirical patterns that have been discovered in the selected empirical evidence and are empirically supported by actual instances of cyber operations in the conflict between Iran and Israel (2010-2026).

A systematic review of documents generated consistent empirical patterns among the selected sources. Specifically, four major categories of unintended consequences were observed: (1) spill-over effects on civilian infrastructure; (2) economic and transnational ramifications; (3) escalation; and (4) proliferation of cyber capabilities. Empirical patterns were discovered inductively from the codes and consistently occurred in cyber-attacks as documented.

Empirical support is strengthened by Table 1, which lists significant cyber incidents between Iran and Israel, along with their intended goals and unintended consequences.

Table 1: Selected Cyber Incidents in the Iran-Israel Conflict (2010–2026)

2010	Israel/US (attributed)	Iranian nuclear facilities	Disrupt uranium enrichment (Stuxnet)	Global malware proliferation; replication of cyber tools; escalation of cyber capabilities	Lindsay (2013); Zetter (2014)
2012	Iran (attributed)	Saudi Aramco (regional spill-over)	Retaliation and disruption	Regional economic disruption; spread beyond the immediate conflict actors	Valeriano & Maness (2015)
2020	Israel (attributed)	Iranian port (Shahid Rajaee)	Disrupt logistics operations	Civilian shipping delays; economic ripple effects	Tabatabai (2020)
2020	Iran (attributed)	Israeli water infrastructure	Disrupt water systems	Risk to civilian health systems; exposure of vulnerabilities	ENISA (2023)
2021-2023	Both actors	Multiple sectors (energy, logistics, data systems)	Strategic signalling and disruption	Persistent low-intensity conflict; normalisation of cyber exchanges	Healey (2022)
2024–2026	Both actors/proxies	Mixed civilian and digital infrastructure	Coercion and retaliation	Increased involvement of non-state actors; diffusion of cyber tools; global systemic risks	Rid (2023); Smeets (2022)

Civilian Infrastructure Spill-over

One of the major insights obtained from this research is that the impacts of cyber-attacks have the tendency to go beyond the initial target due to the lack of intent by the perpetrators to include civilians in the attack. The example of Iran-Israel shows that while the cyber-attacks are initially carried out on strategic and military infrastructures, their impacts extend to other fields such as health facilities, water supplies, transportation, and corporate entities. This spill-over is mostly based on the architecture used in the development of the cyber technology.

Among the major theoretical frameworks utilised in obtaining these insights is the complexity theory that suggests that due to the interconnections and interdependencies among the systems, the effects of cyber-attacks cannot be predicted since a disruption in one element affects another one. Other theories include the theory of unintended consequences in which actions carried out for the purpose of achieving something lead to unexpected results. Hence, the findings contradict the idea that cyber

operations represent the best approach to warfare because even the civilian population is negatively impacted.

The empirical evidence in Table 1, especially the 2020 water infrastructure attack, shows how the disruption planned by the strategy proved dangerous to civilians and other vital services.

Economic Disruption and Transnational Effects

Furthermore, cyber warfare possesses significant economic implications that transcend state boundaries. The attacks carried out by Iran and Israel against each other's finances, energy, and logistics sectors have generated a cascade effect in the international and regional markets. The above example shows how vulnerable the current economies are because they rely extensively on computer systems and immediate data flow.

The recent literature review confirms the assertion that cyber intrusions can bring about threats to the global economy networks (Healey, 2022; ENISA, 2023). It is important to note that cyber warfare does not only comprise a military tactic but also a danger to economic safety. Based on the results obtained from the study, it becomes evident that economic activities can transform into a battlefield in cyber warfare due to their non-military nature. Consequently, it becomes necessary to consider cyber-attacks through the prism of economics and appreciate the importance of economic relations in today's global politics. For instance, the cyber attack conducted against Iranian ports in 2020 brought about shipping problems and economic repercussions in regions beyond the targeted zone.

Escalation Dynamics and Strategic Instability

A closely related finding is that cyber warfare helps to initiate the escalation of attacks. Rather than dissuading the adversary from any further actions, cyber operations provoke the adversary to conduct retaliatory operations against the first side, hence creating an attack and defence loop. As for the current confrontation between Iran and Israel, this has resulted in the creation of what can be referred to as a "shadow war," which involves continuous cycles of cyber operations.

What makes it impossible to apply theories about deterrence to the analysis of cyber operations is that the theories stipulate that an actor should first be able to detect his/her adversary before he/she proceeds with the retaliatory activity. However, this is hardly possible since the operations in question are conducted by an anonymous/ambiguous party (Nye, 2017; Smeets, 2022). Therefore, the practice of cyber warfare neither serves as a means of deterring actors but, on the contrary, creates instability and the likelihood of miscalculations.

One can trace this trend based on the following timeline of events between 2010 and 2026 (see Table 1).

Proliferation and Diffusion of Cyber Capabilities

Cyber warfare might promote the development of capabilities by different parties involved. The release of information and the spread of knowledge related to various cyber tools and hacks, as experienced in the aftermath of the Stuxnet attack, contributed to the proliferation of these capabilities. As seen in the Iran-Israel cyber warfare, the proliferation of cyber capabilities led to the appearance of proxies as well as hackers participating in the cyber wars without any supervision or control at all.

This phenomenon relates to the notion of democratisation of cyber capabilities (Slayton, 2021; Rid, 2023). Cyber tools and capabilities differ from conventional weapons due to the ease with which they can be reproduced and used in cyber conflicts. This aspect means that many actors can engage in cyber warfare and make it more challenging for states to control the dynamics of escalation. Additionally, this observation raises the issue of global implications of cyber warfare due to the spread of capabilities across the globe.

Blurring the Boundary between War and Peace

As stated by the study, the use of cyber warfare leads to the significant blurring of the line between war and peace. When considering the Iran-Israel case, this is because cyber activities never end and usually do not rise above the level of an officially declared act of war. Thus, a state of constant conflict emerges during which hostile behaviour becomes normalised and routine within geopolitics.

Such results align with the conclusions of contemporary authors who argue that cyber warfare undermines established laws and norms (Lindsay, 2020; Nye, 2022). Because cyber activity is ambiguous, it can be hard to attribute blame or respond to such actions while also applying the concepts of sovereignty and defence. This leads to cyber warfare becoming a factor in the transformation of notions of competition, coercion, and warfare.

Psychological and Informational Consequences

Apart from tangible and economic consequences, there are also psychological and informational repercussions resulting from the cyber warfare conducted in the Iran-Israel context. Among them are disinformation campaigns, data breaches, and surveillance activities aimed at influencing public perception and trust. As can be seen in the current Iran-Israel confrontation, cyber operations are increasingly used against information networks.

As is evident from recent studies on the impact of cyber warfare on the creation of the information environment (Rid, 2023), it is essential to understand its implications for cognition and how people view various security risks. It is worth noting that this dimension of cyber confrontation operates in a rather discreet manner, with long-term effects on perception and behaviour.

In general, findings from systematic document analysis indicate that cyber warfare in the Iran-Israel conflict leads to consistent, observable unintended outcomes. They are based on real cases and represent system-level dynamics rather than individual occurrences. To avoid repetition, the results were not included elsewhere in the paper.

Conclusions

The purpose of this paper was to analyse the unexpected consequences of cyber warfare, using the Iran-Israel conflict as an example. As the analysis shows, cyber operations, even when intended to cause as little damage as possible and to ensure precision and control, lead to a wide array of unpredictable and hard-to-control consequences and instead of de-escalating the conflict between Israel and Iran, cyber operations used during the conflict resulted in the disruption of civilian infrastructures, economic reverberations, a cycle of escalations, and an increase in the number of actors with advanced cyber capabilities. The above-mentioned is caused by the specific nature of cyber warfare, which is inherently unpredictable due to characteristics such as stealth and affordability.

On the theoretical level, the paper can be regarded as a contribution to the development of both International Relations and Cybersecurity Studies. Thus, cyber warfare should not be viewed solely through the lens of International Relations and Cybersecurity Studies, since cyber operations can be analysed using frameworks proposed by different theories, such as deterrence, complexity, and the theory of unintended consequences.

The implications of this research on cyber warfare are substantial for policy-making and implementation. First, this research calls into question the common assumption that cyber war is only an instrument used as a last resort in military actions. On the contrary, this research proves that cyber operations introduce ambiguity into the very idea of distinguishing war from peace, resulting in constant interaction that makes governance increasingly difficult. Second, the vulnerability of civilians

and the global economy to cyber warfare makes clear the need to develop new methods of ensuring resilience in the current interdependent environment.

In light of the discussion above, the following recommendations are advanced. First, there is a need to create international guidelines and laws to regulate and punish any form of cyber warfare. Countries should endeavour to protect themselves from any form of cyber attack by acquiring technology and building institutions. In addition, it is necessary to foster international collaboration in addressing any threat emanating from cyberspace. Lastly, policymakers should exercise careful consideration when formulating policies on cyber conflicts to avoid unforeseen negative consequences.

In conclusion, the case study of the relationship between Israel and Iran indicates that, although cyber warfare is a relatively new development in the history of conflict, it has changed the approach to and conduct of conflict and warfare in modern times.

Acknowledgements
It would not be an exaggeration to note the importance of the work of various scholars, institutions, and organisations that contributed greatly to the completion of this paper. The author would like to thank the scholarly community for their contributions to the fields of cyber warfare, international security, and digital conflict, which provided the background for this research.

Moreover, there is no doubt about the significance of the information provided by such renowned and respected institutions dealing with policies and cybersecurity, which enabled the writing of this essay. Their dedication to advancing this area of knowledge is invaluable. Lastly, the author is thankful for the atmosphere of constructive criticism that surrounded the writing process.

References

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

Buchanan, B. (2020). *The hacker and the state: Cyber-attacks and the new normal of geopolitics*. Harvard University Press.

Byman, D. (2023). Iran's regional strategy and proxy warfare. Foreign Affairs. https://www.foreignaffairs.com

Carr, M. (2021). *US power and the internet in international relations: The irony of the information age*. Palgrave Macmillan.

European Union Agency for Cybersecurity (ENISA). (2023). ENISA threat landscape 2023. https://www.enisa.europa.eu

Healey, J. (2022). *Cyber war and systemic risk*. Atlantic Council.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Lindsay, J. R. (2020). *Information technology and military power*. Cornell University Press.

Mazarr, M. J., Priebe, M., Radin, A., & Cohen, N. (2015). *Understanding the gray zone: How states compete below the threshold of war*. RAND Corporation.

Merton, R. K. (1936). The unanticipated consequences of purposive social action. *American Sociological Review, 1*(6), 894–904. https://doi.org/10.2307/2084615

Mitchell, M. (2009). *Complexity: A guided tour*. Oxford University Press.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Nye, J. S. (2022). *Do morals matter? Presidents and foreign policy from FDR to Trump*. Oxford University Press.

Rid, T. (2023). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Schelling, T. C. (1966). Arms and influence. Yale University Press.

Slayton, R. (2021). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security, 45*(4), 72–109. https://doi.org/10.1162/isec_a_00418

Smeets, M. (2022). *No short-cuts: Why states struggle to develop a military cyber-force*. Oxford University Press.

Tabatabai, A. (2020). Iran's evolving cyber strategy. *Survival, 62*(1), 131–150. https://doi.org/10.1080/00396338.2020.1715062

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.

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

Yin, R. K. (2018). *Case study research and applications: Design and methods (6th ed.)*. Sage Publications.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publishers.