Review Paper/Pregledni rad UDC/UDK:355.4:004.6.056
Paper Submitted/Rad primljen: 3. 10. 2022.
Paper Accepted/Rad prihvaćen: 26. 1. 2023.
DOI: 10.5937/SJEM2301038K

Strateška odbrana kao igra sajber bezbednosti

Milan V. Kovačević[1], Đurica M. Iličić[2], Nenad M. Jevtić[3]

[1]Provincial Government of Autonomous Province of Vojvodina, Provincial Secretariat for Economy and Tourism
[2]Ministry of Defence of the Republic of Serbia - Military Medical Academy
[3]Ministry of Defence of the Republic of Serbia – Regional Centre Valjevo

Apstrakt: Trenutno se napadači i branioci bore za pristup i kontrolu informacija u političkoj, ekonomskoj, vojnoj i društvenoj sferi. Vojnim jezikom, podaci su postali virtuelna 'visoka tačka' sa koje se može uticati na bolje upućenog protivnika. Strateška odbrana je postala igra sajber bezbednosti. Međutim, uprkos brojnim tehnološkim rešenjima koja su uvedena za rešavanje ranjivosti sistema, ljudski faktor ostaje najveća pretnja bezbednosti sistema. Ovaj rad, na primeru ukrajinsko-ruskog konflikta, promoviše primenu strateških vojnih koncepata na sajber sukob u cilju boljeg rešavanja dinamičkog izazova kontinuirane interakcije između prilagodljivih i inteligentnih protivnika. Počinje zalaganjem za korisnost vojne paradigme u sajber prostoru, iako bez želje za militarizacijom sajber prostora. Zaključak je da je vojni način razmišljanja, koji je zasnovan na sukobu sa dinamičnim, prilagodljivim protivnicima, pouzdanija strategija od preovlađujuće paradigme „sajber higijene“. Opisano je pet nivoa strateške misli kako bi se povezali ciljevi sa politikom, strategijom, kampanjama i operacijama, taktikama i instrumentima. Svaki nivo strateške misli primenjen je na hipotetički scenario odbrane mreže. Konačno, rad je demonstrirao alternativu tehnološko-centričnim strategijama koje su nedovoljne za borbu protiv protivnika ugrađivanjem strateškog razmišljanja u digitalnu odbranu.

Ključne reči: sajber higijena, sajber ratovanje, konflikt, strateška misao, sajber odbrana

Strategic Defence as a Cyber Security Game

Abstract: Currently, both assaulters and perservers strive to be in a position of access to information, and also control in the field of economics, warfare, and society. Describe in military terms, data has become a virtual 'high ground' from which a more knowledgeable opponent can be influenced. Strategic defence became a cyber security game. However, despite the numerous technological solutions introduced to address system vulnerabilities, the human factor remains the greatest threat to system security. On the example of Ukraine-Russia conflict, this paper promotes the implementation of military strategy concepts to cyberconflict in order to better address the dynamical challenges of continual interaction between conformable and intelligent opponents. It begins by arguing for the adaptability of a military paradigm in cyberspace, though, without a desire for cyberspace's militarization. The conclusion is that the military mindset, which is predicated on clashes with dynamic, adaptable opponents, is a more dependable strategy than the prevalent cyber-hygiene paradigm. Five levels of strategic thought were described in order to connect objectives to policy, strategy, campaigns and operations, tactics, and instruments. Each level of strategic thinking was applied to a hypothetical defence script. Finally, the paper showed a substitute to technocentric strategies that are insufficient to combat the opponent by incorporating strategic thinking into digital defence.

Keywords: cyber hygiene, cyber warfare, conflict, strategic thought, cyber defence

1. Introduction

Beginning during the Second World War, the digitization of information has highly strengthened the association among humans (from the personal to the nation and state levels) and unstructured data, structured information, and intelligence (pieces of information with military or social value) (Unver, 2018). Each aspect of society has gained certain conveniences from information technologies, but it made us dependent on data, which our opponents accepted as a tool to be used *versus* us. Currently, both assaulters and perservers strive to be in a position of access to information, and also control in the field of economics, warfare, and society (Powers & Jablonski, 2015). In warfare terms, information has become an advantage from which a more knowledgeable opponent can be influenced. Currently, the Ukrainian Government is at a tactical drawback compared to Russian Federation, both on the conventional battlefield and in cyber battlefield. Nevertheless, cyber security, particularly at the nation-level, is a pastime of strategy, and Ukraine can invest in long-term which is sought to pay off. Practitioners, academics, policymakers, and the general public in Ukraine are perplexed, both on personal and collective level, by asking of how to protect information (Greminger & Vestner, 2022). Another hindrance is that the opponents do not have a single or even numerous attacking tactics since they can purloin, demolish, repudiate access to, or change information – as well as the systems that hoard, processing, and show it to its purported proprietors.

Digitized data is a man's creation that resides in devices projected and built by engineers. Thus, decision-makers look to the tech-community for solutions to such issues (Cai & Zhang, 2013). Technical proposals can take a variety of shapes. Some of them often show themselves in policymaking spheres, such as that we may abandon the internet as a hole, and replace it with some highly secured alternative. We could create 'impenetrable' software applications, through advanced technologies that make defence easier than wrongdoing (which is not the case at the moment); or we could transfer our security problems to outsourced companies. All of aforementioned concepts sound technically doable, still cannot be implemented on account of numerous reasons. Basically, it is risky to rely only on technological aspects to address fundamental issues (Hammes, 2021).

2. Limits of Tech-Driven Methodologies

Technological basis plays a crucial function in the protection of data. Intruders looking for simple prey can be thwarted by well-designed networks, higher-quality software, and nimble startups. Unfortunately, sometimes well-resourced, professional attackers are on a long-term mission to damage specific, valuable prey, whether for stealing the data or to manipulate (Ogun, 2015). They will persevere until their mission requirements change or they are successful in their mission. Digital perservers might only catch a view of the perpetrator, which is frequently far too late. In contrast to the casualty's point of view, which is typically limited and deficient, professional assailants are tenacious and know precisely what do they aim at (Pomranky, 2010). According to Libicki (2021), the average number of days a triumphant threat group was present on a victim's network before being detected in 2014 was more than two hundred. In one instance, an attacker kept unauthorized access for more than eight years. Even after detection, organizations may invest months attempting to eradicate the intruder.

The foreign hackers continued to plague the US State Department three months after the agency breach. This interrelation between security and cadence is essential for safeguarding cyber resources. Understanding the interaction between attackers and defenders requires an analysis of time intervals, but the security clique does not understand or respect the essence and consequences of this connection. A techno-centric look is preoccupied with still, disposable interactions betwixt assailant and perserver. This might not be a precise depiction of the reality, which is inhabited not by programming code, but by people who have a mind of their own and are able to adjust, grant resources, and create a dynamical resolution in order to achieve objectives (Schneider, 2015). A Digital perserver that ignores such realities does so by increasing risk. The interactive and time-dependent nature of network attack and defence encourages suboptimal security strategies.

The emphasis on 'cyber hygiene' is indicative. This mode encourages good visibility into your own network, slicing and dropping systems that don't have permissions, patching potential vulnerabilities, and improving settings to deter potential attackers from attacking. All of these defensive measures are obligatory and commendable. Nevertheless, they are not enough against adversaries who have the time and assets to adjust to the defences of the victim and overcome them. "Washing cyber hands" is

beneficial for preventing the unfurl of vacuous pathogens, but it is not as effective to more intelligent germs (Ratnaweera & Pivovarov, 2019).

3. Strategic Cyber Defence Ideas

This paper promotes the implementation of conventional warfare strategy concepts to cyberconflict in order to better adapt to the accelerating challenge of a constant interaction ratio between adaptive and intelligent opponents. Conventional combat has traditionally been characterized as a protracted grapple between tenacious opponents (Lucas, 2017). In the late XVIII and early XIX century, the emergence of large armies, modern weapons and clashes, elevated this concept to a higher level. Therefore, military strategists of the 20th century needed to consider far out of the conventional doublet of tactics and strategy. They coded numerous levels of skirmishes over time. In the 80s, the United States Army doctrine characterized several levels of war: strategical, and operation and tactic levels. From Napoleonic battles to Soviet military planning, these drew upon previous writings and lessons learned (Townshend, 2005). National objectives and policy were incorporated into doctrine, despite the fact where term 'strategy' frequently emerged in the prototype's as one of its most important constituents, which can be perplexing (Hoffman, 2016).

Figure 1. Steps in strategic thinking. Adapted from: (Johnson & Clack, 2015).

We contend that decision-makers must have a deeper understanding of the role of technology in strategic thinking; therefore, 'tools' is added as a new layer beneath the tactical layer. Undoubtedly, in physical warfare, 'weapons' are used to inflict kinetic damage. In the digital realm, models age explicitly. In the digital realm, the model demonstrates their strategic position. Too many professionals in digital security believe that tools are the sole focus of defensive action (Sambaluk, 2019). By placing tools at the bottom of the model, the author believes they appear in their correct location. In addition, the expression 'campaign' is included at the operational level in this model. Sometimes, 'campaigns' and 'operations' are used interchangeably, so both terms appear to reduce confusion (Drew, 2020).

This is illustrated in the Figure 1. The policies and objectives of an organization are broad statements that define the desired purpose of the strategic program. Strategy is a plana for how a group can use its resources to reach its goal and policy. Operation, grouped into "campaigns" in this schema, is a sequence of activities that are used to carry out strategies that are followed over days, weeks, months, or even years. (Christiano, 2022). Tactics are the things you do when you meet an opponent one-on-one. They are the basic building blocks of a campaign. Tools are the digital things an actor uses to put plans into action. All of these parts have to work together for success to happen (Roach, 2015). Before

explaining how these five levels can improve digital defence, it's important to mention that this paper does not propose to "militarize" cyberspace, which is a worry of numerous professionals. For instance, Chesterman (2011) wrote that the military had "prioritized one national security objective -- more espionage and the ability to carry out attacks - above all others." This question was seen by journalists as a question of "nonsensical militarization" of it, "active equipping with military forces and a different spectrum of defence means" or, say, "adaptation realized for the needs of military use." Although the author of the paper does not generally agree with these assumptions, there is a need to combine strategic thought with the goal of militarization. of today's actual computer intrusions.

4. Using the Strategic Model for Traditional Security

In today's digital age, where technology permeates every aspect of our lives, ensuring the security of our digital assets has become of utmost importance. Cybersecurity has emerged as a critical field to protect individuals, organizations, and nations from the ever-evolving threat landscape. To effectively address cybersecurity challenges, a strategic approach is necessary (Fielder, Panaousis, Malacaria et al., 2016). First it is needed to understand the Strategic Model: The strategic model is a systematic framework used to develop and implement effective strategies in various domains, including cybersecurity. It involves a holistic approach that encompasses analysis, planning, execution, and evaluation of security measures. The model aims to align security objectives with organizational goals and adapt to changing threat landscapes. Key Components of the Strategic Model in Cybersecurity are, at the first place a Risk Assessment. It is a crucial component of the strategic model is conducting a comprehensive risk assessment. This involves identifying and analysing potential threats, vulnerabilities, and potential impacts. By understanding the risks, organizations can prioritize their security efforts and allocate resources effectively. Furthermore, security policies and procedures: developing robust security policies and procedures is vital for protecting digital assets.

These policies define guidelines for access control, data protection, incident response, and other essential security measures (McGraw, Miques & West, 2013). By establishing clear protocols, organizations can ensure consistency and compliance in their security practices. Incident Response Planning: Being prepared for cyber incidents is essential in mitigating their impact. The strategic model emphasizes the development of an incident response plan, which outlines the necessary actions to be taken in the event of a security breach. This includes detection, containment, eradication, and recovery processes, along with communication and coordination strategies (Skarga-Bandurova, Kotsiuba & Velasco, 2021). People are often the weakest link in cybersecurity. Therefore, the strategic model emphasizes the importance of security awareness and training programs. By educating employees about potential threats, safe practices, and the significance of cybersecurity, organizations can enhance their overall security posture (ISACA, 2015).

The strategic model recognizes the dynamic nature of cybersecurity and the need for continuous monitoring and improvement. Organizations should regularly assess their security measures, monitor network activity, and implement necessary updates (Shumard, 2015). This proactive approach helps identify emerging threats and adapt security measures accordingly. The strategic model ensures that cybersecurity efforts align with broader organizational goals and objectives. By integrating security considerations into the overall business strategy, organizations can protect their critical assets and maintain business continuity (Kavyn, Bratsuk & Lytvynenko, 2021). By conducting risk assessments and prioritizing security efforts, the strategic model helps organizations allocate resources effectively.

This ensures that investments in cybersecurity are directed where they are most needed, maximizing the return on investment and minimizing potential losses. The strategic model's emphasis on incident response planning enables organizations to respond swiftly and effectively to security incidents (Caelli, 2012). With predefined protocols and clear roles and responsibilities, organizations can minimize the impact of breaches and swiftly restore normal operations. Through security awareness and training programs, the strategic model fosters a cybersecurity-conscious culture within organizations. This leads to increased vigilance, improved adherence to security practices, and better overall resilience against cyber threats. As cyber threats continue to evolve in complexity and scale, adopting a strategic model for traditional cybersecurity becomes increasingly critical (Yadron, 2014). By leveraging the components of risk assessment, security policies, incident response planning, security awareness, and continuous monitoring, organizations can develop a proactive and resilient cybersecurity posture. The strategic model provides a comprehensive framework that aligns security objectives with organizational goals, leading to improved protection of digital assets and enhanced overall

cybersecurity resilience (Rindell, Hyrynsalmi & Leppänen, 2018). However, information security research has been almost exclusively focused on technical problems, and efforts to enhance information security have been software- or hardware-centric (Bella, Curzon & Lenzini, 2015). There have been few attempts to resolve computer users, despite the fact that they are the greatest security vulnerability in information systems. Despite the numerous technological solutions introduced to address system vulnerabilities, the human factor remains the greatest threat to system security (Saflanu & Twum, 2016).

5. Cyber Security Lacking a Plan

It is extremely important to understand how the basic strategic principles of cyber security can be adapted and fully implemented in order to better protect important digital assets. Attacks by ruthless criminal groups and groups that represent threats to the national interests of the state greatly compromise numerous private organizations and seek to alienate their intellectual property, including various trade secrets, highly sensitive and confidential commercial data, as well as numerous other digital assets (Collins & McCombie, 2012). It should be pointed out that the traditional security model of 'tools and tactics' is undeniably characterized by extremely suboptimal communication and extremely poor coordination between different levels of management, the board of directors and members of the security team. The one under the direct management of the CISO, is more than determined to decisively confront the adversary.

Their first step involves taking decisive tangible actions, such as recruiting new staff, developing modern capabilities, adopting an entirely new strategy, or acquiring an entirely new software application (Justice & Sample, 2022). The CISO will develop an argument for and against based on an immediate ROI assessment that includes the very cost of the proposed initiative, the amount of money we should save (provided almost everything goes well) and the inevitable precise mathematical calculation of the total risk undertaken by the enterprise. If by any chance the CEO or the board expresses a desire to clarify the reasoning, the CISO will be obliged to provide information and will demonstrate an approach using various tools and tactics to save invested money and reduce the level of risk. Management has two options. They will either approve the proposal or ask the CISO to redesign the approach. This cycle in its original form requires that the budget be reviewed until management realizes that the more money, they spend on ROI needs and on network security itself, the more money they actually save later.

At the very end of the cycle, management comes to the conclusion that security is far more important in preventing losses than generating revenue, and they become extremely disengaged (and of course dissatisfied) with protecting their very important digital assets. In doing so, they admit that their organization is just one of many whose boards are not fully aware of current strategy and have never actually participated in an attempt to formulate a serious strategy.

6. Strategical Perspective of Security in Cyber Domain

Contrary to such a point of view, a strategic cyber security program in reality begins with the precise definition of one or more program objectives, rather than the tools or tactics themselves. First, from a strategic point of view, the CISO receives executive support for the realization of these goals. In order to achieve the stated goal, the CISO must in some way include all levels of strategic thinking, starting with the board itself and inevitably the CEO. Everyone must have an active participation. The CISO understands very well that security is an uncertain journey, not the final destination itself, and that the aforementioned relationship building is complex and requires the ability to translate two extremes, between technical and non-technical vocabularies (Subramanian, 2020). The CISO tries to regulate the objectives of the program as precisely as possible, and this primarily refers to the company's digital security programs. The CISO, Board and CEO agree by acclamation that the goal of this brand-new policy is to preserve and protect intellectual property, sensitive trade secrets, and valuable data and that the goal is to fully minimize loss due to a possible intrusion. Such a worded statement implies that everyone is able to recognize the impossibility of completely stopping all adversaries and almost all attacks, especially those when they are actually actors belonging to nation states and certain well-organized criminal organizations.

The immediate goal of this exercise is to inevitably reach a consensus on a non-technical, proclaimed program goal. Consensus can very easily be reached without any in-depth technical discussion, but it is

important to point out that the CISO must ensure that all set goals, chosen policies and chosen strategies are technically feasible. The CISO can practically confidently collaborate with his carefully selected security team to plan all important operations and campaigns and, if the need arises, acquire new security tools and create new strategies to facilitate their execution. Everyone makes a decision together with the aim of conducting a full network security monitoring operation, which is defined as collecting data and summarizing indications and warnings in order to immediately detect and respond to potential intruders (Fuentes-Garcia, Camacho & Macia-Fernandez, 2021). The security team has the authority to initiate a long-term, strategic process of looking for various complex hostile cyber-attack campaigns, which include all known to date as well as those future, unknown intrusion patterns.

The CISO, board, and CEO are tasked with agreeing that rapid detection, timely response, and decisive containment of cyber threats is that expected second goal of the program. This objective ensures that the threat is not defeated if the perimeter defences are breached. As long as they have the ability to react before the attacker completes his ultimate goal, the defenders can take the upper hand. Therefore, the security team will develop appropriate strategies for radical and rapid identification of various compromises, determining their real nature, attribution and, most importantly, have the ability to devise a plan to effectively prevent the attacker from trying to realize his mission.
At the immediate tactical level of inevitable one-on-one confrontations with an adversary—analogous to wartime battles—the security team will be forced to make a number of very important decisions, such as whether to expel the intruder immediately or to wisely and calmly observe the intruder for a while in order to gathered very valuable information about the nature and source of the attack (AlKadheeb, Bhattachariia & Perl, 2022). Some tactics necessarily incorporate the use of certain tools or techniques, which would be analogous to, say, the crew of the Star Trek franchise switching their handheld phasers between settings to different modes that include the "stun" and "kill" positions. It should be noted that the adversary has some say in what happens, but from the company's perspective, important program goals, key policies and set guidelines should be drawn up in order to regulate this entire very important process.

7. The Applicability of Campaigns

The campaign, which seems to be working successfully at the operational level itself, is essential to the overall concept and to the inevitable success of the strategic security program as a whole. It should be noted that the maturity of a security program can be carefully assessed by the immediate attention that the CISO and his or her security team devote to the immediate development of the campaign itself, as well as by a broad understanding of the level of progress and analysis of the campaign itself by superior senior management. When talking about specific campaigns themselves and evaluating them in terms of sheer sophistication and breadth of impact, careful discussions with other executives, the board, and other key stakeholders are crucial. The CEO should have the ability to talk in detail about the various threat actors behind the campaigns, including their means and motivations, as well as provide visual examples of each campaign and how the security team directly responded to them. In addition, the very important term 'campaign' fits more than well into existing non-technological business operations such as marketing and, say, sales campaigns.

Despite these efforts, it should be emphasized that the number of cyber-attacks is constantly increasing (Shandler & Gomez, 2022). Individual attacks implemented include ghost everything from say a suspicious TCP packet to a very unusual computer port, then some random suspicious SQL query and sinister 'phishing' email (Verma & Shri, 2022). A more in-depth discussion of individual attacks is of somewhat limited value. A legitimate question arises, how can one give oneself the right to imagine a fully credible programmatic goal to counter the dizzying number of several tens of billions of attacks (Verma & Shri, 2022)? The optimal strategy necessary to organize primary threats and immediate threat actors into logical campaigns actually lies somewhere in no man's land. This is potentially the most effective method for a business organization or nation-state to combat a highly cunning interactive and above all highly adaptive adversary.

8. Ukrainian Cybersecurity Strategies

The new Ukrainian government, which has extremely hostile relations with Russia and is involved in an especially long-lasting conflict, appears to be the target of numerous extensive and orchestrated cyber-attack campaigns. The only possible way to counter such a brutal offensive campaign, in the opinion of the author, is to equally conduct a determined and unwavering defensive campaign. In April

2015, the notorious security firm Looking Glass revealed a large-scale and well-orchestrated "Operation Armageddon", which it saw as a well-known pattern of cyber-espionage (activities going back to 2013) designed to give Russia a "tangible military advantage" in intends to target the Ukrainian government, then law enforcement and various military officials who appear to be of interest to the intelligence services (Jasper, 2020). As expected, the researchers found a direct correlation between large-scale digital attacks and the current ongoing conflict, as well as an almost alarming combination of all known forms of cyber-espionage, brutal physical warfare and geopolitics itself. Reports from reputable security firms such as Trend Micro and FireEie have exposed Russian campaigns dubbed "Operation Pawn Storm" and "APT28". According to FireEie, APT28 appears to have narrowly and cunningly targeted individuals associated in any way with European security organizations.

Organizations such as the North Atlantic Treaty Organization (NATO) and the Organization for Security and Cooperation in Europe (OSCE) stand out here. These are precisely those organizations that the Russian government has seen for many years as an existential threat to its security. It should also be noted that some Russian non-state actors such as CyberBerkut play an active role in the cyber fight against the NATO pact and targets of interest in Ukraine (Lilli, 2022). At the end of March 2014, the group launched extensive, highly sophisticated attacks involving so-called distributed denial-of-service (DDoS) attacks on the primary website of the NATO pact, the website of the CCD COE and the website of the NATO Parliamentary Assembly. In the same year, in October 2014, on the eve of the parliamentary elections in Ukraine, extensive and well-planned and coordinated DDoS attacks were launched on the website of the Central Election Commission of the country, into which election materials were poured from all parts of the country. The group also targeted US military structures operating in Ukraine, publishing highly classified documents concerning the secret transfer of Western military equipment to strengthen the country's defence power (Sakva, 2015).

The nature of national security requirements is above all strategic and they do not change very often. it should be emphasized the fact that what can to some extent be considered a legitimate problem of national security, states will dedicate enormous human and material resources in order to achieve their goals. At the same time, they will not hesitate to use a very wide range of methods and forms of attack. The country will most certainly not surrender after one or even after several dozen or even hundreds of disastrous tactical engagements. On the contrary, it will regroup and break through even the strongest defences. Nation-states differ greatly from individuals and even well-organized hacker groups such as the famous Anonymous, countries such as Russia also qualify as so-called advanced actors in terms of security threats (Kose, 2021). That designation "advanced" indicates the adversary's immediate ability to operate across the spectrum of different computer intrusions, both in terms of target and intensity.

Depending on the immediate location of the target, they can use well-known vulnerabilities, or they can try to improve their approach by continuously researching new vulnerabilities and developing tools that adapt to further exploitation (Iakoviv, 2018). it should be emphasized that every country, including Russia itself, has a key and very significant ability to adapt, and this is one of the very important reasons why close monitoring of threats is crucial at all levels of strategic thinking. This actually means that whenever a failed intrusion attempt is attributed to some so-called advanced actor, the security team can be more than sure that this seemingly defeated adversary will return with some new inventive technique and possibly a new, far more sophisticated campaign.

9. Conclusion

The Government of Ukraine is presently at a pitfall against Russian Federation, in the conventional battlefield as well as in the cyber area. Still, security in cyber space, particularly at the national level, is a game of strategy, and Kyiv can make long-term investments that will pay off. This paper has argued that digital defence requires strategic consideration. First, it argued for the implementation of a conventional militaristic paradigm in cyber area, even though they without wanting to militarize it. We argued that the military mindset, which is predicated on a dynamical clash, adaptable enemies, is far more well-grounded strategy compared to prevalent cyber hygienic paradigm. Furthermore, the paper recounts the 5 levels of strategy thinking, connecting objectives to policies, strategies, manoeuvres and activities. Every level of strategical thinking was applied to a hypothetic intertwining defence script. This paper showed a surrogate to techno-centric strategies, insufficient to combat the enemy by incorporating strategic thinking into digital defence. During a war, Ukraine is an obvious prey for many cyber attackers and initiatives. The only way to beat them is to take an equally aggressive defensive stance in cyberspace.

Literature

1. (Bill) Caelli, W. J. (2012). Cyber Warfare – Techniques, Tactics and Tools for Security Practitioners. *Computers & Security*, *31*(4). https://doi.org/10.1016/j.cose.2012.02.010
2. AlQadheeb, A., Bhattacharyya, S., & Perl, S. (2022). Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior. *Array*, *14*. https://doi.org/10.1016/j.array.2022.100146
3. Bella, G., Curzon, P., & Lenzini, G. (2015). Service security and privacy as a socio-technical problem: Literature review, analysis methodology and challenge domains. *Journal of Computer Security*, *23*(5). https://doi.org/10.3233/JCS-150536
4. Cai, S. Z. & Zhang, Q. F. (2013). *Information Technology Applications in Industry, Computer Engineering and Materials Science*. Trans Tech Publications Ltd.
5. Charles Townshend. (2005). *The Oxford History of Modern War: Vol. New updated ed*. OUP Oxford.
6. Collins, S., & McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, *7*(1). https://doi.org/10.1080/18335330.2012.653198
7. Cristiano, F. (2022). The Blurring Politics of Cyber Conflict : A Critical Study of the Digital in Palestine and Beyond [Lund University]. In *Lund Political Studies MECW: The Middle East in the Contemporary World*.
8. Drew II, J. V. (2020). The Army's Gap in Operational-Level Intelligence for Space as Part of Multi-Domain Operations. *Military Review*, *100*(1), 70–79.
9. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*. https://doi.org/10.1016/j.dss.2016.02.012
10. Fuentes-Garcia, M., Camacho, J., & Macia-Fernandez, G. (2021). Present and Future of Network Security Monitoring. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3067106
11. Greminger, T. & Vestner, T. (2022). The Russia-Ukraine War's Implications for Global Security: A First Multi-issue Analysis. GCSP. https://dam.gcsp.ch/files/doc/gcsp-analysis-russia-ukraine-war-implications?_gl=1*134rvid*_ga*MTI1MTI3OTcwLjE2NTU3MjkyMTY.*_ga_Z66DSTVXTJ*MTY2OTMwMzAyMS4xODAuMS4xNjY5MzA0OTQyLjAuMC4w
12. Hammes, T. X. (2021). The Tactical Defense Becomes Dominant Again. *JFQ: Joint Force Quarterly*, *103*, 10–17.
13. He, H. (2021). Research on Xi Jinping's Important Exposition on Information Technology Education. *E3S Web of Conferences*, *275*. https://doi.org/10.1051/e3sconf/202127503059
14. Hoffman, J. (2016). *Future of the U.S. Army: Background and the National Commission's Report*. Nova Science Publishers, Inc.
15. ISACA. (2015). State of Cybersecurity : Implications for 2015. *CyberSecurity Nexus*.
16. Jasper, S. (2020). Russian Cyber Operations : Coding the Boundaries of Conflict. Georgetown University Press
17. Justice, C., & Sample, C. (2022). Future Needs of the Cybersecurity Workforce. *International Conference on Cyber Warfare and Security*, *17*(1). https://doi.org/10.34190/iccws.17.1.33
18. Kavyn, S., Bratsuk, I., & Lytvynenko, A. (2021). Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France. *Teisė*, *121*. https://doi.org/10.15388/teise.2021.121.8
19. Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.
20. Kose, J. (2021). Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage. *ISSA Journal*, *19*(4).
21. Lilly, B. (2022). Russian Information Warfare : Assault on Democracies in the Cyber Wild West. Naval Institute Press.
22. Martin Libicki. (2021). *Cyberspace in Peace and War, Second Edition: Vol. Second edition*. Naval Institute Press.
23. McGraw, G., Miques, S., & West, J. (2013). Building security In maturity model V. In *Faulkner Information Services* (Issue October).
24. Nicholas Michael Sambaluk. (2019). *Conflict in the 21st Century : The Impact of Cyber Warfare, Social Media, and Technology*. ABC-CLIO.
25. Ogun, M. N., & NATO Science for Peace and Security Programme. (2015). *Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses*. IOS Press.

26. Pomranky, R. A. (2010). *Experimental evaluation of computer-aided tele-operation (CATO) and computer-aided robotic manipulation (CARMAN) technology [electronic resource] / Regina A. Pomranky ... [et al.]*. Aberdeen Proving Ground, MD : Army Research Laboratory, 2010
27. Powers, S. M. & Jablonski, M. (2015). The Real Cyber War : The Political Economy of Internet Freedom. University of Illinois Press
28. Ratnaweera, H., & Pivovarov, O. A. (2019). *Physical and Cyber Safety in Critical Water Infrastructure*. IOS Press.
29. Rindell, K., Hyrynsalmi, S., & Leppänen, V. (2018). Aligning security objectives with agile software development. *ACM International Conference Proceeding Series*, *Part F147763*. https://doi.org/10.1145/3234152.3234187
30. Roach, K. (2015). *Comparative Counter-Terrorism Law*. Cambridge University Press.
31. Safianu, O., Twum, F., & B., J. (2016). Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. *International Journal of Computer Applications*, *143*(5). https://doi.org/10.5120/ijca2016910160
32. Sakwa, R. (2015). Frontline Ukraine : Crisis in the Borderlands. I.B. Tauris.
33. Schneider, J. (2020). A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem. *Washington Quarterly*, *43*(2), 159–175. https://doi.org/10.1080/0163660X.2020.1770970
34. Shandler, R., & Gomez, M. A. (2022). The hidden threat of cyber-attacks–undermining public confidence in government. *Journal of Information Technology and Politics*. https://doi.org/10.1080/19331681.2022.2112796
35. Shumard, C. (2015). *CISOs Face Tough Challenges When Procuring Security Technologies*, Tenable Network Security. Available at: http://www.tenable.com/blog/cisos-face-tough-challenges-when-procuring-security-technologies. Accessed 2nd July, 2022.
36. Simon Chesterman. (2011). *One Nation Under Surveillance : A New Social Contract to Defend Freedom Without Sacrificing Liberty*. OUP Oxford.
37. Skarga-Bandurova, I., Kotsiuba, I., & Velasco, E. R. (2021). Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.614337
38. Subramanian, O. (2020). Moving from blocker to enabler: cloud security and the modern CISO. *Computer Fraud and Security*, *2020*(10). https://doi.org/10.1016/S1361-3723(20)30106-8
39. Ünver, H. A. (2018). Politics of Digital Surveillance, National Security and Privacy. Centre for Economics and Foreign Policy Studies. http://www.jstor.org/stable/resrep17009
40. Verma, A., & Shri, C. (2022). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision*. https://doi.org/10.1177/09722629221074760
41. Yadron, D. (2014). *Symantec Develops New Attack on Cyberhacking.* Wall Street Journal. Available at: http://www.wsj.com/articles/SB10001424052702303417104579542140235850578 Accessed 2nd July, 2022.
42. Yakoviv, I. (2018). Cybernetic model of the advanced persisten threat. *Collection "Information Technology and Security," 6*(1). https://doi.org/10.20535/2411-1031.2018.6