Open Access Library Journal
2022, Volume 9, e9003
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Taming the Shrew of Rising Cyber-Warfare

Festus C. Obi[1], Alaba M. Oludare[2]

[1]East Texas Baptist University, Marshall, TX, USA
[2]Mississippi Valley State University, Mississippi Valley State, MS, USA
Email: fobi@etbu.edu

How to cite this paper: Obi, F.C. and Oludare, A.M. (2022) Taming the Shrew of Rising Cyber-Warfare. *Open Access Library Journal*, **9**: e9003.
https://doi.org/10.4236/oalib.1109003

Received: June 15, 2022
Accepted: December 25, 2022
Published: December 28, 2022

Abstract

Cyber-warfare is rising astronomically. With the advancement in technology comes increased scope of victimization. Individuals, organizations, and countries are not left out in the ever-expanding list of victims. State and non-state cyber-warriors are not sparing any entity that makes itself vulnerable. This article examines the historical and definitional dimensions of cyberwarfare as well as the factors responsible for the victimization of both states and non-state victims. It also proffers solutions for "taming the shrew" of the ever-expanding menace of cyber warfare.

Subject Areas

Politics

Keywords

Cyber-Warfare, Cybersecurity, Cyberbullying, Information War, Cyber-Attack

1. Introduction

The rise of cyber-warfare keeps individuals, organizations, and countries apprehensive. Actors, both state and non-state, seem determined to wield their power over unsuspecting and ill-prepared targets. The underlying factors for the rise of cyber-warfare across the globe include, among others, the quest for economic and political dominance. The focus of this article is a historical and contemporary examination, as well as definitional dimensions, of cyber warfare or attacks. Also, the article will explore efforts by organizations and countries to beef up their cybersecurity. The article will end up with recommendations that will help individuals, businesses, and nations combat the threats of cyber warfare. As nuclear warfare is heavily diminished, cyber-warfare is the novel method for cudgeling organizations and countries into compliance. Cyber-warfare is also

known as information war (IW) or cyber-attack (CA).

According to Pawar (2022) [1], there is a cyber-attack every 39 seconds globally. For instance, in 2020, the Federal Bureau of Investigation (FBI) received more than 2,000 complaints of cybercrime. Individuals, business entities, and nations are resorting to information technology (especially World Wide Web) as a means for settling scores, enriching themselves, stealing other businesses' secrets, and gaining a military advantage over other nations, enemy nations. Since the Corona Virus Disease (COVID) there has been about a 60% spike in the risk of a data breach suffered by internet users (Pawar, 2022) [1]. He also stated that one in 10 small businesses suffers a cyber-attack each year, a ransomware attack occurs every 14 seconds, and over 90% of successful cyberwarfare against businesses occurs through phishing, while 37% of all cybercrime attacks against firms are via phishing. Additionally, the largest Distributed Denial of Service (DDoS) attack in 2018 was against the software depository platform GitHub. About 1.3 TB (terabyte) of data was transferred every second. DDoS is a strategy by cyber warriors to prevent clients from accessing the websites of legitimate businesses. The global loss to cybercrime is currently more than $2 trillion.

Before cyber-warfare became the most effective means of destroying opponents' economic, financial, and military capabilities through internet attacks, individuals and nations fought with clubs, spears, bows and arrows, muskets, high-caliber guns and rifles, and nuclear arms. But since the end of the Cold War in the early 1990s and the popularization of personal computers and superhighway access, advanced computer users have resorted to a convenient way of launching paralyzing warfare against enemies from remote locations. Vulnerable individuals, businesses, and nations have become victims of cyber-warfare at some points. Many more are falling victim because of the convenience of this style of warfare. Pawar (2022) [1] added that hackers need only $1 to obtain a malware kit and only $25 to obtain at least a million compromised emails or passwords. 91% of cyber-attacks originate with a spear phishing email. Non-state actors use cyber-warfare or cyber-attack to extort from their victims which are mainly organizations with the help of malware and ransomware. State actors aim at stealing trade and defense secrets of competitors and enemy nations, while also pushing to attack their targets' critical infrastructure.

Recent attacks on companies and countries further highlight the obviousness of cyber-warfare and the seeming inability to defend against them. It is also hard to predict when the attack will occur. Several precautionary measures against cyber-warfare have proved inadequate. For instance, in August of 2012, the world's biggest oil producer known as Saudi Aramco suffered a viral attack that compelled the company to go offline to purge thousands of computers that comprised its information database. Iran's oil ministry had its computers attacked with the Flame malware. The 2012 attack on Iran's oil ministry's computers was traced to the United States and Israel (Porsche III *et al.*, 2012) [2]. Before then Iran's nuclear facilities were attacked by what looked like the Stux-

net worm between 2009 and 2010. Target and Neiman Marcus databases were attacked in late 2013. Over sixty million customers had their personally identifying information (PII) breached. Cyberwarfare has greater potential for success and inflicts more damage than ordinary nuclear war on the economic, technological, and military capabilities of an enemy. By the end of 2025, global financial loss to cybercrime will be about $10.5 trillion.

According to Porsche III *et al.* (2012) [2], recent cyber-warfare has been against the energy industries, a pointer to the vulnerability of the computer networks of the victims and the capabilities of their attackers. Cyber-warfare is borderless. It takes place from remote locations and does not necessarily have to be launched from a computer. We live in a wireless world. That means that an attacker could launch debilitating worms from any wireless device so long as they have the know-how. Cyber-warfare does not require military knowledge; it requires computer knowledge and the ability to create and transmit worms or viruses that could damage the opponents' capabilities. Hjortdal (2011) [3] noted that cyber-warfare could be accidental and not intentional. Where the attacker has no definitive enemy in mind but is out to attack whoever is vulnerable; that attack would still be considered intentional. Unintentional breaches would normally result from simple negligence, inattention, or lack of education with no general intent to attack anyone. For example, these include unintentional mistakes or omissions by employees who are not properly trained to protect sensitive information against accidental or unlawful destruction or accidental loss, alteration, or unauthorized use (Smedinghoff, 2008) [4].

Hathaway *et al.* (2012) [5] attempted to provide a subtle comparison of cyber-attack, cybercrime, and cyberwarfare. Cyber-warfare occurs at the individual, industrial, and national levels or what Hoisington (2009) [6] called "state and non-state actors" (p. 439). Countries like China, India, Iran, Israel, North Korea, Pakistan, Russia, and the United States among others are fully engaged in the war, according to Billo and Chang (2004) [7]. This paper will examine the rise of cyber-warfare and the ramifications of its prosecution. It will also recommend strategies for dealing with it. Cyber-warfare could be traced to the then Soviet Union which in a bid for an upper hand in its nuclear arms race with the United States hired a German computer internet expert in 1972 to hack into the military computers of the United States. Since then thousands of attacks have been launched against many opponents all over the world. In 1998, 3000 Chinese hackers launched thousands of attacks against Indonesia as a protest against the anti-China demonstrations that occurred in the country.

2. Definition and Origin of Cyber-Warfare

There are many definitions of cyber-warfare. Therefore, scholars are not agreed on one single definition. Its difficulty stems from various conceptualizations of the word cyber-warfare. This does not mean that cyber-warfare cannot be defined. Joyner and Lotrionte (2001) [8] offered an instructive explanation. They

defined cyber-warfare as an information war or attack that can "severely damage or disrupt national defense or other social services and result in serious harm to the public welfare" (p. 858). Cyber-warfare, consequently, is intended to inflict harm on individuals, corporations, and nations or governments. The ubiquity of computers and the interconnectedness of global cyberspace, the blurring of boundaries, and the accessibility of the internet have made cyber-warfare an easy way to launch attacks against opponents. Countries like China have adopted the doctrine of cyber-warfare as an acceptable and advantageous stratagem of war. This is because these countries perceive this stratagem as putting them at an asymmetrical advantage against militarily stronger countries like the United States.

Those engaged in cyber-warfare have two objectives in mind. One, they want to keep their information technology inviolable. Two, they intend to disrupt and exploit others' technological abilities and potentials to their advantage. It is a warfare that lacks the form and characteristics of conventional war. The motivation could be retaliation but, in most cases, the reason lacks retaliatory underpinning. Its motivation is to exploit the strength of a stronger opponent by rendering the opponent weak. Cyber-warfare could be defined finally as the malicious swapping of positions initiated mostly by a weaker opponent against a stronger opponent. So, cyber-warfare is an offensive war. It often leads to retaliation and counter-attacks by an opponent that has been violated. Shackelford (2009) [9] highlighted the convenience of cyber-warfare in comparison with nuclear war. The fact that cyber-warfare does not need costly expenditure on its arsenals makes it a ready weapon. According to him, cyber-warfare should be seen through the prism of offense and defense, and defense and offense.

Knapp and Boulton (2006) [10] explicated that cyber-warfare or information warfare, a terminology attributed to Dr. Thomas Rona in 1976, aims at causing political, security, criminal, economic, and military consequences. Libicki (1995) [11] defined information warfare by offering seven forms that the war takes, command and control warfare, intelligence-based warfare, electronic warfare, hacker warfare, economic information warfare, cyber-warfare, and psychological warfare. Cyber-warfare, however, encompasses all the other components outlined above.

Cyber-warfare did not come out of the blues. It is a phenomenon that has its roots in the desire of nations to engage adversaries in non-nuclear warfare. Although non-state participators have escalated cyber-warfare, countries like China, Iran, Russia, and others see cyber-warfare as an asymmetric war strategy. Asymmetric war strategy means the scheme of a weak state to do battle with a stronger state by turning the stronger opponent's strength into vulnerability (Breen & Geltzer, 2011) [12]. Countries such as the United States are well advanced in technology but this technological advancement presents areas of vulnerabilities that opponents could capitalize on.

This points to the fact that individuals might decide to carry out cyber-warfare

against governments or corporations and vice versa. Instances abound of cyber-wars unleashed on governments as well as corporations. In 2008, Estonia was attacked to a point of paralysis. This compelled the North Atlantic Treaty Organization (NATO), a military consortium of former allied countries during the World War 2 to change its policies to reflect the threats and urgency of action against cyber-warfare. In 2009, Georgia was attacked "cyberly" during its war against Russia over South Ossetia. Similarly, Stuxnet a worm was released into Iranian computers with a suspected motive of disrupting Iran's nuclear enrichment. Israel and the United States were accused of releasing the Stuxnet virus (Trautman & Ormerod, 2017) [13].

Cyber-warfare is a real war that should not be taken lightly, according to O'Connell (2012) [14]. She pointed out that many countries including the United States have approached cyber-warfare with a military mindset. Such countries have created commands charged with the responsibilities of deterring cyber-warfare by launching proactive offensive cyber-warfare and also for creating a multi-layered cyber defense that would be impregnable to an opponent. Cyberwarfare has become our current arms race. Countries like China have been at the forefront of cyber warfare and espionage, launching thousands of attacks against nations, businesses, and media perceived as an enemy. O'Connell (2012) [14] observed that countries no longer wait to be attacked before defending themselves. Most countries are on the offensive, they do not wait to be attacked before going after perceived enemies. The fear of cyber-warfare has also led to increased espionage as countries have broadened their spying network to include everyone and everything.

Definitively, a persistent dilemma exists in the area of conceptualizing cybercrime, cyber warfare, and cyber-attack based on existing literature. For instance, Robinson *et al.* (2015) [15] rightly questioned Billo and Chang's (2004) [7] definition of cyber warfare as organized along nation-state boundaries, offensive, and defensive operations, and using computers to attack other computers or networks through electronic means. He claims that Billo and Chang (2004) [7] suggest that the attacks are organized along nation-state boundaries. This definition appears to be rudimentary and places a locational limitation on cyber warfare that may not exist. Robinson *et al.* also noted various problems with other definitions provided in extant literature including the Oxford English Dictionary (2013) [16], Parks and Duggan (2011) [17], Carr (2012) [18], and Cornish *et al.* (2012) [19] to be debatable.

Robinson *et al.* [15] then proceeded to resolve the definitional dilemma by providing a methodological procedure that identifies the actor and intention for incidents of cyber warfare. He explained that the actor and intent definition model posits that all unwarranted cyber situations arise from the premise that an actor is launching an attack with a harmful intention. Cyber-attack can reasonably be defined as an act in space that can reasonably be expected to cause strategic, economic, psychological, reputational, and physical damage and more. Robinson and associates then proceeded to offer a tautological explanation of

cyberwar to involve the declaration of war by one nation-state against another where cyber war is the exclusive means used to fight a cyber war. To the extent that a kinetic attack such as an airstrike is used, then it is not cyber warfare but a war where cyber warfare was used. Robinson *et al*. conceded that the ultimate decision on whether cyberspace is a warfighting domain is unlikely to be resolved by academia and should be deferred to the Military who are the experts in the art of warfighting (pg. 91).

2.1. Motivations and Means of Cyber-Warfare

What causes cyber-warfare? Could it have been undertaken as a mere pleasure trip? Similar to every other war, there is always a real or imaginary cause of cyber-warfare. According to Billo and Chang (2004) [7], there are different motivations for different countries in their launch of cyber-warfare. However, there are common threads that run through each motive, especially with certain countries such as China, India, Iran, North Korea, Pakistan, and Russia. The primary motivation for launching cyber-warfare is often to inflict incalculable financial and material losses on the opponent.

Billo and Chang (2004) [7] also found out in their study that countries referenced here aim at information take-down of an opponent by paralyzing its internet connection, disrupting communication, compromising data, impeding commerce, and debilitating the information and technological infrastructure of the adversary. China, for instance, knows that it cannot match many countries in nuclear warfare but has the human capital to engage its adversaries in cyber-warfare. Its official doctrine of cyber-warfare states a determination to raise as many cyber warriors as possible to engage its enemies asymmetrically, using China's nuclear weaknesses as an advantage for gaining information technological superiority over its stronger opponents. This entails being proactive and offensive in its tactical approach to combatting its enemies through the sheer overwhelming population of cyber warriors.

In its confrontation with Pakistan over Kashmir and Pakistan's ability to launch nuclear and technological warfare, India has made the pursuit of cyber security and warfare a part of its military doctrine. In 1998, India began a 10-year information plan that will give it an advantage over its opponents (Billo and Chang, 2004) [7]. This is also the case with other countries that the authors studied. The countries all want to use the information superhighway to deal with their opponents, thereby making cyber-warfare assume the same importance as nuclear warfare, if not more.

John H. Herz (1950) [20] argued that uncertainty and bounded rationality (Inkster, 2013) [21] drive many individuals, corporations, and countries to insecurity. The produced insecurity creates feelings of threats that the fearful tend to fight against. Most of the security threats that lead to information warfare stem from uncertainty and insecurity within one's bounded rationality. At the moment, China and the United States, India and Pakistan, Russia and United States, Israel and Iran, and Iran and the United States are all caught in the web of

uncertainty and insecurity emanating from real or perceived threats. This feeling of insecurity pushes each of these countries to defend themselves against the other's security threats or cyber-warfare and engage in tactical offensive moves aimed at accumulating greater power and advantage.

Cyberspace is an open space. O'Connell (2012) [14] pointed to the interconnectedness of computers on the information superhighway. This international open space of the internet makes access to computers easy. It is just like an open door or closed but unlocked door which makes entry unhindered. So, according to scholars like O'Connell (2012) [14], and Billo and Chang (2004) [7], the internet creates access to intruders and thieves whose intention is to wreak havoc on their victims. This state of the internet is the biggest weapon for cyber warfare. Individuals and countries that engage in cyber-warfare or attacks watch out for the vulnerabilities of an information infrastructure that give them unfettered access to personally identifiable information, trade secrets, military and defense strategies, and security policies. The means of cyber-warfare is the internet connection. Also, an information security vulnerability is another means through which attackers launch cyber warfare. This then indicates that information security is vital to ward off cyber-warfare success. Cyber-warfare is inevitable, especially with the frontier expanding to include non-state warriors. Advanced knowledge of information superhighway and how information securities work and their vulnerabilities are all it takes for an opponent to launch cyber-warfare against an adversary. Warriors use malware, viruses, or worms to disrupt opponents' data tables and corrupt the hard drive, the operating system, and all files available in the system. They also steal vital information if they can gain access.

2.2. Military and Civilian Warriors

Cyber-warfare was initially regarded as military warfare. It was engaged by countries to gain a military advantage over their opponents. When the Soviet Union began a cyber-attack in 1972, it did so to undermine America's nuclear superiority. It also had a mind to shift the turf of the war. Knapp and Boulton (2006) [10] in their review of literature on cyber-warfare from 1990 to 2005 found that corporations are increasingly becoming victims of this war. They explained that there has been a transition of cyber-warfare from being a military non-bloody weapon to commercial and industrial espionage and destruction. This transformation of the scope of the war has far-reaching implications not only for business entities and their customers but also for understanding the phenomenon. Cyber-warfare has become a critical societal dilemma. Cronin (2002 [22], 2002 [23]) argued that because cyber-warfare was first fought as a military and defense maneuver, scholars failed to address the civilian dimension of the war.

Though countries and their military arms have been targeted by cyber-warriors, victims have been mainly corporations and private organizations. Low entry security can account for one of the reasons for the prevalence. Over-dependence

on information technology by corporations has exacerbated their victimhood. The internet is overwhelmingly used for industrial espionage, organized crime, public opinion management, and against individuals and small businesses. With millions of people globally becoming increasingly computer savvy, the rate of cyber-warfare rises.

3. Trends of Cyber-Warfare

Existing literature shows that there are innumerable incidents of computer-related incidents of cyber-warfare. Many of these incidents target individuals and civilian organizations. To compound this prevalence is the failure of victims of cyber-warfare to report the breaches.

According to Pawar (2022) [1], only 10% of cybercrimes are reported to law enforcement in the United States. Also, it is estimated that by 2027, cybercrimes against the United States will account for 50% of all global cybercrimes. Sometimes, some corporations are unaware of their victimhood until government law enforcement agencies bring the occurrences to their knowledge. The first death recorded as a result of a ransomware attack occurred in Germany in 2020 in a hospital in Dusseldorf due to IT failure from a ransomware attack (Pawar, 2022) [1]. A survey by the Federal Bureau of Investigation (FBI) in 2002 showed that 90% of cyber-warfare attacks were known by victims but only 34% reported them to law enforcement agencies (see Knapp & Boulton) [10]. To say that thousands of cyber-warfare take place daily is repeating the obvious. The question that users of the internet and information highway constantly ask is, how to forestall cyber-attacks. Some attacks may not be prevented but how does one keep some of the enemies at bay?

An expanding trend of cyberwarfare is the activities of initial access brokers (Maor, 2022) [24]. An IAB is a cyber actor that sells access to a company to other bad actors on the dark web. Recent cyber-attacks on a leading automotive company and Cisco are traced to IABs. A U.S. prison had a ransomware attack that paralyzed the CCTV cameras and automatic doors in that institution in January of 2022. After weeks of ransomware attacks, Costa Rica declared a state of emergency on April 17 (Reed, 2022) [25]. A series of cyber-attacks crippled government exports, pension payments, taxes, Social Security services, and Covid-19 testing (Maor, 2022) [24]. Experts are of the view that as more workloads are being deployed to the cloud by 2025, cyberattacks on cloud service areas, applications, and infrastructure will rise. Maor [24] also noted that cybercriminals are using cloud technology to disseminate malware that hijacks cloud environments, issues commands, and steals data. Attackers are not new to using cloud services to "deliver malicious office documents and host malicious payloads on legitimate cloud platforms like MediaFire, Blogger, and GitHub" (p. 3). The UK's 4783/million internet user victims of cybercrime are the highest in the world. The United States is the next with 1494/million internet user victims, showing a decrease of 13% from the 2020 figure (Griffiths, 2022) [26]. Conversely, Greece

has witnessed the largest decrease in cyber victimization down by 75% since 2020. China (485%) and South Korea (1007%) represent account breaches of 14,157,775, and 1, 669,124 during the second and third quarters of 2022. For the same periods, Sri Lanka had 1,440,432 (−99%), Myanmar 17,887 (−82%), and Iraq 15,113 (−78%) fewer account breaches. In 2021, Asian countries suffered the most cyber attacks (26%) followed by Europe (24%), and North America (23%) (Griffiths, 2022). The five top countries on the National Cyber Security Index (NCSI) for the year 2022 are Greece (96.10%), Lithuania (93.51%), Belgium (93.51), Estonia (93.51%), and the Czech Republic (92.21%). The index measures the following in ranking the various countries of the world:

- Identification of national level of cyber threats;
- Identification of cyber security measures and capacities;
- Selection of important and measurable aspects;
- Development of cyber security indicators;
- Grouping of cyber security indicators (NCSI, n.d.) [27].

Many companies and countries are spending heavily on cyber security in response to cyber warfare. In 2020, cybersecurity expenditure was $205.4 billion and is estimated to reach $367.3 billion by 2026. For instance, Microsoft spends about $1 billion on cybersecurity every year besides the cost of acquisitions in cybersecurity. JPMorgan Chase spends about $600 million on cybersecurity services every year. Cybersecurity liability insurance costs will reach $20 billion in three years. Some companies pay up to $500,000 to legitimate hackers to test the resilience of their information systems and databases. Still, about 68% of companies do not have cybersecurity defenses, while 25% are planning to invest in cybersecurity.

4. Recommendations

4.1. Wholesome Stakeholder Involvement in Cyber Security

The need for organizational cyber-security strategies cannot be over-emphasized. Stakeholders should build solid information architecture that has the capabilities to withstand all forms of cyber-ware. This can be achieved by hiring knowledgeable and certified information security personnel, conducting a periodic risk assessment of information platforms, and training employees on the risks of vulnerability and precautions against intended breaches.

4.2. Creation of Multi-Layered Cyber Defense

Tucker (2004) [28] recommended the creation of architecture of technological high walls with hidden armed guards for information protection. There is also a need for a multi-layered defense mechanism created around each country's information platform. Though this may not be enough, it goes a long way to help. It might be difficult to ward off all cyber-warfare but failure to do so compounds the problems. Just as many countries are writing their military doctrines to center around cyber-warfare security, every business and country should develop

information security strategies and policies that will guide how they engage this serious global enemy.

4.3. Establish Cyber Security Policy Committee

Establish a cyber security policy committee for each country to be managed by cyber security experts, business leaders, law enforcement agencies, and policy-makers. The committee should develop a doctrine that is implemented and evaluated periodically to ensure that the greatest defense against cyber-warfare is proactivity.

4.4. Create Offline Data Backup System

Due to the high rate of cyber warfare resulting in data breaches, it is imperative to have a reliable and secure offline data backup system to mitigate the impact on operations and assets from loss or destruction. It is also very important to provide a working incident response program including plans, policies, procedures, standards, and education for all stakeholders. That is anticipating the inevitability of an attack and doing all necessary to deter it no matter when it comes.

5. Conclusion

The problems associated with cyber-warfare, cyberattacks, and cybercrime cannot be solved exclusively within the purview of a single discipline. It requires a multi-disciplinary approach. For instance, cyber defense and attribution problems are technical issues that may be dealt with within the core sciences but are also fraught with political, legal, and social aspects including the role of people. Likewise, effective laws for curbing cyber-warfare require not only legal input but also technical, military, and law enforcement responsibilities (Robinson, *et al.*, 2015). The effort for lawmaking and enforcement against should not only be interdisciplinary, but it must also involve a coordinated effort of nations on the global level (Dogrul, *et al.*, 2011) [29], and the adoption of cyber peacekeeping mechanisms in the future as the spate of cybercrimes, cyberattacks, and cyber warfare continue to rise (Robinson *et al.*, 2018) [30].

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Pawar, P. (2022) 50+ Alarming Cybersecurity Statistics 2022 Facts and Trends That Users Need. EnterpriseAppsToday. https://www.enterpriseappstoday.com

[2] Porche III, I.R., Sollinger, J.M. and McKay, S. (2012) An Enemy without Boundaries. *Proceedings Magazine*, **138**, 1-6.

[3] Hjortdal, M. (2011) China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security*, **4**, 1-24. https://doi.org/10.5038/1944-0472.4.2.1

[4] Smedinghoff, T.J. (2008) Information Security Law: The Emerging Standard for Corporate Compliance. IT Governance Ltd., Ely.

[5] Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J. (2012) The Law of Cyber-Attack. *California Law Review*, **100**, 817-885.

[6] Hoisington, M. (2009) Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. *Boston College International and Comparative Law Review*, **32**, 439-454. https://doi.org/10.2139/ssrn.1542223

[7] Billo, C. and Chang, W. (2004) Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation-States. Institute for Security Technology Studies at Dartmouth College, Hanover.

[8] Joyner, C.C. and Lorionte, C. (2001) Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International*, **12**, 825-865. https://doi.org/10.1093/ejil/12.5.825

[9] Shackelford, S.J. (2009) From Nuclear War to Netwar: Analogizing Cyber-Attacks in International Law. *Berkeley Journal of International Law*, **27**, 192-251.

[10] Knapp, K.J. and Boulton, W.R. (2006) Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments. *Information System Management*, **23**, 76-87. https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92675.8

[11] Libicki, M.C. (1995) What Is Information Warfare? National Defense University Institute for National Strategic Studies, Washington DC. https://doi.org/10.21236/ADA385640

[12] Breen, M. and Geltzer, J.A. (2011) Asymmetric Strategies as Strategies of the Strong. *Parameters*, **41**, 41-55. https://doi.org/10.55540/0031-1723.2565

[13] Trautman, L.J. and Ormerod, P.C. (2017) Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things. *University of Miami Law Review*, **72**, 761. https://doi.org/10.2139/ssrn.2982629

[14] O'Connell, M.E. (2012) Cyber Security without Cyber War. *Journal of Conflict & Security*, **17**, 187-209. https://doi.org/10.1093/jcsl/krs017

[15] Robinson, M., Jones, K. and Janicke, H. (2015) Cyber Warfare: Issues and Challenges. *Computers & Security*, **49**, 70-94. https://doi.org/10.1016/j.cose.2014.11.007

[16] (2013) Oxford English Dictionary. Oxford University Press, Oxford.

[17] Parks, R.C. and Duggan, D.P. (2011) Principles of Cyber Warfare. *IEEE Security & Privacy*, **9**, 30-35. https://doi.org/10.1109/MSP.2011.138

[18] Carr, J. (2012) Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media, Inc., Sebastopol.

[19] Cornish, P., Livingstone, D., Clemente, D. and Yorke, C. (2012) On Cyber Warfare.

[20] Herz, J.H. (1950) Idealist Internationalism and the Security Dilemma. *World Politics*, **2**, 157-180. https://doi.org/10.2307/2009187

[21] Inkster, N. (2013) Conflict Foretold: America and China. *Survival*, **55**, 7-28. https://doi.org/10.1080/00396338.2013.841802

[22] Cronin, B. (2002) Information Warfare. *Library Journal*, **127**, 54.

[23] Cronin, B. (2002) Information Warfare: Peering inside Pandora's Postmodern Box. *Library Journal*, **50**, 279-294. https://doi.org/10.1108/EUM0000000005600

[24] Maor, E. (2022) Cyberattacks 2022: Key Observations and Takeaways. Forbes Technology Council Post. https://forbes.com

[25] Reed, J. (2022) Costa Rica State Emergency Declared after Ransomware Attacks. Security Intelligence. https://securityintelligence.com

[26] Griffiths, C. (2022) The Latest 2022 Cyber Crime Statistics (Updated December 2022). AAG IT. https://aag-it.com

[27] National Cyber Security Index (2022) NCSI Development Process. https://ncsi.ega.ee/methodology

[28] Tucker, T.E. (2004) Leveraging Protection Mechanisms to Provide Defense in Depth. In: Whitman, M.E. and Mattord, H.J., Eds., *Management of Information Security*, Course Technology, Boston, p 408.

[29] Dogrul, M., Aslan, A. and Celik, E. (2011) Developing International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. 2011 *IEEE* 3*rd International Conference on Cyber Conflict*, Tallinn, 7-10 June 2011, 1-15.

[30] Robinson, M., Jones, K., Janicke, H. and Maglaras, L. (2018) An Introduction to Cyber Peacekeeping. *Journal of Network and Computer Applications*, **114**, 70-87. https://doi.org/10.1016/j.jnca.2018.04.010