SOFT DIGITAL WEAPONS AND KAKISTOSCRYPTOCRACY

Srirath GOHWONG[1]
1 Department of Political Science and Public Administration, Faculty of Social Sciences, Kasetsart University, Thailand; srirath.g@ku.th

ARTICLE HISTORY
Received: 19 April 2024 **Revised:** 3 May 2024 **Published:** 17 May 2024

ABSTRACT
The objectives of the study were to elaborately investigate the state-of-the-art of soft digital weapons (SDWs), examine their relationship with kakistoscryptocracy, and propose the application of governmental power market-ing as a solution to their negative effects. The methodology employed was documentary research. The findings revealed that the state-of-the-art of SDWs were categorized into three groups: predators-oriented usage, parasites-oriented usage, and parasitoids-oriented usage. Next, the relationship between SDWs and Kakistoscryptocracy could be elaborately explained in three issues-SDWs and cybersecurity, kakistoscryptocracy, and the intersection of SDWs and kakistoscryptocracy in cyber warfare. Lastly, two vital strategies, internal and external, could be implemented to effectively address the challenges posed by SDWs and Kakistoscryptocracy, through the establishment of high-level multi-stakeholder partnerships (MSPs).
Keywords: Soft Digital Weapon, Kakistoscryptocracy, Government Power Market-ing

CITATION INFORMATION: Gohwong, S. (2024). Soft Digital Weapons and Kakistoscryptocracy. *Procedia of Multidisciplinary Research, 2*(5), 51.

INTRODUCTION

The emergence of disruptive, malicious-purpose-oriented coding technology since 2010 has brought about a new phase of virtual warfare. Soft Digital Weapons (SDW), notably malware, have emerged as novel threats to information security. The first official SDW, Stuxnet, was secretly developed by the U.S. in 2010 to sabotage Iran. Since then, a variety of digital weapons have been invented covertly by diverse entities, both state and non-state actors (such as cyber-criminals). These SWDs can impose severe harm to their victims, including public, private, and people entities, from data gathering and espionage to outright sabotage. They inevitably lead to a concerning trend in current cyber warfare. Concurrently, the unthinkable emergence of Kakistoscryptocracy has added another layer of complexity to the tense issue. These non-state actors, including individuals, firms, and even hedge funds, can compromise traditional state sovereignty and conduct illegal activities for personal gains, e.g. money laundering, with Non-Governmental Cryptocurrencies (NGCs). Moreover, the net states, or giant tech firms like Google, Yandex, VKontakte, and Facebook usually operate in state-based and stateless-based areas, making this tense situation much more difficult to hold them accountable. The convergence of SDWs and kakistoscryptocracy obviously represents a formidable challenge in the digital economy, necessitating high-level multi-stakeholder partnerships (MSPs) among governments, firms, people, etc. to maintain sustainably security, sovereignty, and ethical conduct in the digital settings (Particularly thanks to Bjola and Kornprobst, 2024; Carlin, 2018; Deibert, 2013; Ferrag, Kantzavelou, Maglaras, and Janicke, 2024; Gohwong 2017a, 2017b, 2019, 2023a, 2023b; Greenberg, 2019; Jenkinson, 2022; Kello, 2017; Nel, 2017; Whitman and Mattord, 2018; Zetter, 2014). **No previous research has explored the relationship between soft digital weapons and kakistoscryptocracy. To effectively address this knowledge gap, the objectives of the study were to explore the state-of-the-art of soft digital weapons, to investigate on how non-state actors used soft digital weapons for personal gain under kakistoscryptocracy, potentially impacting state sovereignty economy, and society, and to apply market-ing of governmental power to diminish the negative impacts.**

LITERATURE REVIEWS

Kakistoscryptocracy

In 2023, Srirath Gohwong innovatively introduced the term “Kakistoscryptocracy”. It systematically provided a clear scenario where non-state actors, including individuals, firms, and hedge funds, highly influenced three domains, including state-based, stateless-based (with underground websites, NGCs, and pirate agencies), and net states (e.g. Facebook, and Microsoft, in both actual and virtual worlds using various IT tools like AI, TOR, and Web 3.0 (including blockchain and the metaverse). These non-state actors obviously surpassed state sovereignty by doing unlawful activities via NGCs for personal benefits. Gohwong effectively proposed tech ambassadors and corsairs as solutions of this issue (Gohwong, 2023a, 2023b).

Cyberwar and Soft Digital Weapon

Cyber war was a specific term, dedicated to maliciously using computer networks and the internet as intangible weapons, launching attacks against enemy states or agencies to disrupt or damage critical information infrastructure (CII). The actors ranged from state actors (e.g. the United States, China, Russia, Iran, Israel, and North Korea) to non-state actors (such as hackers, terrorist organizations, criminal firms, and individuals). The motivations for these involved actors widely ranged from espionage, sabotage, and national security for nation-states, to economic gain, political or social causes, and destructive intent for non-state actors. One of the key characteristics of cyber war was that it was quite easy to enter because anyone with an inexpensive computer and internet access could commit it effectively. Attackers could stay anonymous, and their attacks could be very damaging. However, it was hard to tell the difference between cybercrime and cyberwar, which made it quite difficult to set up effective

rules for cyber activities. The increase in cyber war significantly led to more spending on defense and digital weapons (both hard and soft) and wide debates about whether using cyber weapons was ethical. Since cyber war was still new, all possibilities of cyber attacks were impossibly defined. One prominent tool in this context was the Soft Digital Weapons (SDWs), which were significant threats under Advanced Persistent Threats (APTs). Their popularity was driven by their existence as code. Hence, they were inexpensive and easily developed, compared to traditional weapons. They were also used anonymously, making it difficult to attribute attacks and hold attackers accountable. In addition, their users and motivations were the same as the cyber war. These weapons mainly focused on malware, e.g. viruses, worms, trojans, ransomware, and spyware. They initially aimed to compromise the CIA triangle by stealing sensitive data, modifying or corrupting data, and preventing authorized users from accessing data or systems. Soft digital weapons, first seen with Stuxnet in 2010, could be effectively delivered through phishing emails, malicious website downloads, or infected USB drives. Their possible victims widely varied from individuals and firms to CII and even government agencies. The impact of a soft digital weapon could range from mild disruption to widespread data breaches or even physical damage (Particularly thanks to Abaimov and Martellini, 2017; Abrams, 2022; Adams, 2015; Allhoff, Henschke, and Strawser, 2016; Arquilla, 2021; Asatryan, 2023; Bjola and Kornprobst, 2024; Bob and Evyatar, 2023; Buchanan, 2020; Carlin, 2018; Carr, 2012; Chapple and Seidl, 2023; River, 2019; Clarke and Knake, 2011, 2019; Davis, 2021; Deibert, 2013; DiMaggio, 2022; Dinniss, 2012; Dragos Inc., 2017; Ferrag, Kantzavelou, Maglaras, and Janicke, 2024; Forest, 2022; Galeotti, 2022; Gohwong, 2017a, 2017b, 2019, 2023a, 2023b; Green, 2015; Greenberg, 2019; Hill, Greenberg, Jeong, Mac, and Cagle, 2015; Jameson, 2022; Jenkinson, 2022; Kaplan, 2017; Kello, 2017; Kokas, 2023; Libicki, 2021; Ma, 2021; Maurer, 2018; Menn and Satter, 2021; Miller, 2020; Nester, 2019; Oladimeji and Kerner, 2023; Pelson, 2021; Porche III, 2020; Relia, 2015; Rosenzweig, 2013; Sambaluk, 2020, 2022; Scott, 2017; Springer, 2017, 2020; Stoddart, 2022; U.S. Department of Defense, Strategic Studies Institute, United States Army War College, Department of Homeland Security, Federal Bureau of Investigation, 2017; Valeriano and Maness, 2015; Valeriano, Jensen, and Maness, 2018; Whyte and Mazanec, 2023; Whitman and Mattord, 2018; Winterfeld and Andress, 2013; Zetter, 2014).

Governmental Power Market-Ing in the VU-CHAOS World

In 2023, the Governmental Power Market-Ing (GPM) in the VU-CHAOS World was an avant-garde concept, elaborately developed by Jermsittiparsert, K., Gohwong, S., Pavapanunkul, S., and Mahittichatkul, N. It originally showed how governments intelligently exploited market-ing to build and sustain their own powers. They elaborately explored various important aspects of governmental power, e.g. gerontocracy, hidden agenda behind government development, sources and status of governmental power, strategies employed in governmental power market-ing, influences on governmental buying behavior, major implications for controlling governmental power market-ing, criteria for assessing its effectiveness, and strategic measures for enduring sustainable power marketing. Last, they innovatively provided insights into strategies for sustainable government branding and power market-ing (Jermsittiparsert, Gohwong, Pavapanunkul, Mahittichatkul, 2023).

RESEARCH METHODOLOGY

This research made thorough use of comprehensive documentary analysis. The data were meticulously gathered from a variety of current sources, including books, and peer-reviewed articles.

RESEARCH RESULTS

The state-of-the-art of soft digital weapons

The state-of-the-art of SDWs, as shown in Table 1, could be explained by the analogy between the pattern of predator insects' exploitation of their victims and SDWs, as described by Gohwong in 2017. Predator insects intensively exploited their victims in three ways: by killing them for feeding, sucking blood, or laying their eggs in or on their hosts for their offspring to consume. Drawing an analogy from predator insects, the application of soft digital weapons could be easily categorized into three groups: predators-oriented usage, focusing on sabotage; parasites-oriented usage, targeting espionage (data theft) and ransomware; and parasitoids-oriented usage, aiming to destroy hard drives after obtaining sensitive data (Gohwong, 2017b). According to Table 1, most of them (with 9 malware, 56.25%) were predators-oriented usage, including Stuxnet, Dark Seoul, Spear-phishing, BlackEnergy, Spear-phishing, StoneDrill, NotPetya, WannaCry, Triton/Trisis, and the Colonial Pipeline Ransomware Attack. Followed by parasites-oriented usage (with 5 malware, 31.25%), there were as follows: a variant of the Shamoon, PowerShell, Browser Exploitation Framework (BeEF), Ryuk, and the SolarWinds Supply Chain Attack. Lastly, the parasitoids-oriented usage (with 2 malware, 12.5%) were Shamoon and Shamoon 2.

Table 1 The state-of-the-art of SDWs

No.	Name	Year	Possible Sponsor	Target
1	Stuxnet	2010	US	Iran's nuclear plant
2	Shamoon	2012	Iran	Saudi Aramco, the joint U.S.-Saudi Arabian oil company
3	Dark Seoul	2013	North Korea	South Korea
4	a variant of the Shamoon	2014	Guardians of Peace (GOP) + North Korea	Sony Pictures
5	Spear-phishing	2014	N/A	a German steel mill
6	BlackEnergy and Spear-phishing	2015 2016	Unknown (Dmytro Oleksiuk - the inventor) alliance of criminal groups	Ukraine
7	PowerShell	2016	N/A	users of PowerShell
8	Browser Exploitation Framework (BeEF)	2016	N/A	many public and private organizations such as * European Union education diversification support agency * Russian foreign trade management organization * Brazilian music instrument retailer * Algerian University's online course platform * Indian military technology school
9	Shamoon2	2017	Iran and Yemen	Three government agencies and four private sector companies in Saudi Arabia + Middle East
10	StoneDrill	2017	Iran and Yemen	European targets
11	NotPetya	2017	Sandworm - a Russian hacker group	Ukrainian government, businesses worldwide
12	WannaCry	2017	North Korea	Hospitals, businesses worldwide
13	Triton/Trisis	2018	N/A	Critical infrastructure (industrial control systems)
14	Ryuk	2019	N/A	Businesses worldwide
15	SolarWinds Supply Chain Attack	2020	N/A	Government agencies, private companies
16	Colonial Pipeline Ransomware Attack	2021	DarkSide	US energy infrastructure

Source: Asatryan (2023), Carlin (2018), Dragos Inc. (2017), Gohwong (2017b), Greenberg (2019), Menn and Satter (2021); Miller (2020), Oladimeji and Kerner (2023)

The relationship between SDWs and Kakistoscryptocracy

The relationship between SDWs and Kakistoscryptocracy could be elaborately explained in three issues (Particularly thanks to Abaimov and Martellini, 2017; Abrams, 2022; Adams, 2015; Allhoff, Henschke, and Strawser, 2016; Arquilla, 2021; Asatryan, 2023; Bjola and Kornprobst, 2024; Bob and Evyatar, 2023; Buchanan, 2020; Carlin, 2018; Carr, 2012; Chapple and Seidl, 2023; River, 2019; Clarke and Knake, 2011, 2019; Davis, 2021; Deibert, 2013; DiMaggio, 2022; Dinniss, 2012; Dragos Inc., 2017; Ferrag, Kantzavelou, Maglaras, and Janicke, 2024; Forest, 2022; Galeotti, 2022; Gohwong, 2017a, 2017b, 2019, 2023a, 2023b; Green, 2015; Greenberg, 2019; Hill, Greenberg, Jeong, Mac, and Cagle, 2015; Jameson, 2022; Jenkinson, 2022; Kaplan, 2017; Kello, 2017; Kokas, 2023; Libicki, 2021; Ma, 2021; Maurer,

2018; Menn and Satter, 2021; Miller, 2020; Nester, 2019; Oladimeji and Kerner, 2023; Pelson, 2021; Porche III, 2020; Relia, 2015; Rosenzweig, 2013; Sambaluk, 2020, 2022; Scott, 2017; Springer, 2017, 2020; Stoddart, 2022; U.S. Department of Defense, Strategic Studies Institute, United States Army War College, Department of Homeland Security, Federal Bureau of Investigation, 2017; Valeriano and Maness, 2015; Valeriano, Jensen, and Maness, 2018; Whyte and Mazanec, 2023; Whitman and Mattord, 2018; Winterfeld and Andress, 2013; Zetter, 2014).
First, SDWs inevitably became important tools for both state and non-state actors. These SDWs were not only intangible and intelligent but also inexpensive and easily developed, making them easily accessible to a wide range of actors. For example, the use of Stuxnet in state-sponsored attacks, the deployment of ransomware that targeted specific entities such as hospitals for maximum disruption, and the creation of underground marketplaces on the dark web where SDWs were unlawfully bought and sold using NGCs, all strongly indicated the disruptive potential of SDWs in compromising the CIA triangle.
Next, the rise of Kakistoscryptocracy obviously allowed non-state actors to use many advanced IT tools, including AI, TOR, Web 3.0, and blockchain, to intentionally surpass traditional state sovereignty and arbitrarily engage in illegal activities for personal gain or political agendas. For example, the use of Monero and its family, e.g. MoneroC, Monero Gold, MoneroV, and Monero Classic, strongly facilitated money laundering and other unlawful transactions, bypassing traditional state-based financial controls. Furthermore, the creation of avatars in a metaverse platform to easily trick users into revealing sensitive information or downloading SDWs hidden in the game content. This explicitly showed how Kakistoscryptocracy made these SDWs much more dangerous.
Lastly, the intersection of SDWs and Kakistoscryptocracy indicated the evolving nature of cyber threats and the challenges faced by governments, organizations, and individuals in defending against them. State-sponsored cyber warfare, such as the use of sophisticated malware to launch technical attacks and disinformation campaigns, exemplified how SDWs could be employed to achieve strategic objectives and rapidly erode adversaries. Moreover, the increasing convergence of cyber warfare with traditional military operations, as discussed in the book, titled "Cyberwarfare: Information Operations in a Connected World," strongly emphasized the need for comprehensive strategies to counter the threats posed by SDWs and the actors behind them.

DISCUSSION & CONCLUSION

Two crucial approaches, internal and external, can be done to effectively address SDWs and Kakistoscryptocracy via GPM. **First,** GPM can be highly employed the Weimer and Vining's measure of establishing rules (Weimer and Vining, 2011). For instance, governments can utilize their own authority and resources to elaborately enact comprehensive cybersecurity policies and regulations, as suggested by Abaimov and Martellini (2017), Adams (2015), and Allhoff et al. (2016). These policies can include highly stringent measures for information security, including data protection, encryption standards, and penalties for cybercriminal activities. Moreover, governments can largely extend their intervention to the regulation of emerging advanced technologies and platforms that smoothly facilitate the widespread of SDWs. Drawing from insights provided by Arquilla (2021) and Asatryan (2023), they can implement measures to monitor and regulate the use of AI, TOR, Web 3.0, and blockchain technologies. **Lastly,** governments can regulate technologies that spread SDWs. They can monitor and control the use of AI, TOR, Web 3.0, and blockchain technologies. They can also use their influence via diplomatic and economic tools, e.g. tech ambassadors, in the global market to strongly encourage responsible behavior among tech firms and individuals to successfully reduce the externality from SDWs and Kakistoscryptocracy. This could be done by rewarding firms that prioritize cybersecurity and penalizing those involved in cybercrimes.

In conclusion, addressing this complex challenge greatly requires high-level multi-stakeholder partnerships and a set of comprehensive strategies, encompassing both internal governmental policies and external diplomatic and economic measures (such as tech ambassadors), to effectively lessen the high risks posed by SDWs and Kakistoscryptocracy.

REFERENCES

Abaimov, S., & Martellini, M. (2017). *Cyber Arms: Security in Cyberspace*. CRC Press.

Abrams, A. B. (2022). *China and America's Tech War from AI to 5G: The Struggle to Shape the Future of World Order*. The Rowman & Littlefield Publishing Group, Inc.

Adams, J. A. (2015). *Cyber Blackout: When the Lights Go Out—Nation at Risk*. 1st ed. FriesenPress.

Allhoff, F., Henschke, A., & Strawser, B. J. (2016). *Binary Bullets: The Ethics of Cyberwarfare*. Oxford University Press.

Arquilla, J. (2021). *Bitskrieg: The new challenge of cyberwarfare*. Polity.

Asatryan, D. (2023). *Ryuk Ransomware: Data Protection Strategies*. Retrieved from https://spin.ai/blog/ryuk-ransomware-data-protection-strategies/.

Bjola, C., & Kornprobst, M. (2024). *Digital International Relations: Technology, Agency and Order*. Routledge.

Bob, Y. J., & Evyatar, I. (2023). *Target Tehran: How Israel Is Using Sabotage, Cyberwarfare, Assassination-and Secret Diplomacy-to Stop a Nuclear Iran and Create a New Middle East*. Simon & Schuster.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Carlin, J. P. (2018). *Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat*. PublicAffairs; Illustrated edition.

Carr, J. (2012). *Inside cyber warfare*. 2nd ed. O'Reilly Media, Inc.

Chapple, M., & Seidl, D. (2023). *Cyberwarfare: Information Operations in a Connected World*. 2nd ed. Jones & Bartlett Learning.

Clarke, R. A., & Knake, R. K. (2011). *Cyber War: The Next Threat to National Security and What to Do about It*. Ecco.

Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press.

Davis, E. V. W. (2021). *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*. Rowman & Littlefield Publishers.

Deibert, R. J. (2013). *Black code: Inside the battle for cyberspace*. Signal.

DiMaggio, J. (2022). *The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*. No Starch Press.

Dinniss, H. H. (2012). *Cyber warfare and the laws of war*. Cambridge University Press.

Dragos Inc. (2017). *TRISIS Malware: Analysis of Safety System Targeted Malware [version 1.20171213]*. Retrieved from https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf.

Ferrag, M. A., Kantzavelou, I., Maglaras, L., & Janicke, H. (2024). *Hybrid Threats, Cyberterrorism and Cyberwarfare*. CRC Press.

Forest, J. J. F. (2022). *Digital Influence Mercenaries: Profits and Power through Information Warfare*. Naval Institute Press.

Galeotti, M. (2022). *The Weaponisation of Everything: A Field Guide to the New Way of War*. Yale University Press.

Gohwong, S. (2017a). *Digital Weapons*. In A paper presented in the 3 rd National and International Conference on Education Research and Social Development, Rangsit University, Thailand on (Vol. 28).

Gohwong, S. (2017b). *Soft Digital Weapons as Predator Insects*. In A paper presented at the 4th International Conference on Security Studies, Bangkok, Thailand (Vol. 20).

Gohwong, S. G. (2019). Deep Web: A Residual of e-Public Administration. *Asian Political Science Review, Asian Political Science Review, 3*(1).

Gohwong, S. (2023a). Kakistoscryptocracy. *Asian Political Science Review, 7*(1).

Gohwong, S. (2023b). Russian Net States and Their Roles in Russia. *Procedia of Multidisciplinary Research, 1*(11), 11.

Green, J. A. (2015). *Cyber Warfare: A multidisciplinary analysis*. Routledge.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Hill, K., Greenberg, A., Jeong, S., Mac, R., & Cagle, S. (2015). *Unmasked: The Man Behind The Silk Road*. Forbes.

Jameson, G. (2022). *Cyber Wars: The Battle for Your Data*. WebStores Ltd.

Jenkinson, A. (2022). *Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare*. 1st ed. CRC Press.

Jermsittiparsert, K., Gohwong, S., Pavapanunkul, S., & Mahittichatkul, N. (2023). *Governmental power market-ing in the VU-CHAOS world*. PA: IGI Global.

Kaplan, F. (2017). *Dark Territory: The Secret History of Cyber War*. Simon & Schuster.

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Kokas, A. (2023). *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*. Oxford University Press.

Libicki, M. C. (2021). *Cyberspace in Peace and War*. 2nd ed. Naval Institute Press.

Ma, W. (2021). *The Digital War: How China's Tech Power Shapes the Future of AI, Blockchain and Cyberspace*. 1st ed. Wiley.

Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.

Menn, J., & Satter, R. (2021). *Pipeline hackers say their aim is cash, not chaos*. Retreived from https://www.reuters.com/business/energy/statement-suspected-us-pipeline-hackers-say-they-dont-want-cause-problems-2021-05-10/.

Miller, L. (2020). *Ransomware Defense for Dummies, Cisco*. 2nd Special Edition. John Wiley & Sons, Inc.

Nel, D. (2017). Multi-sector stakeholder partnerships as a mechanism for creating public value. *African Journal of Public Affairs*, 63-79.

Nester, W. (2019). *Putin's Virtual War: Russia's Subversion and Conversion of America, Europe and the World Beyond*. Frontline Books.

Oladimeji, S., & Kerner, S. M. (2023). *SolarWinds hack explained: Everything you need to know*. Retrieved from https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know#:~:text=Who was responsible for the,is behind the SolarWinds attack.

Pelson, J. (2021). *Wireless Wars: China's Dangerous Domination of 5G and How We're Fighting Back*. BenBella Books.

Porche III, I. R. (2020). *Cyberwarfare: An Introduction to Information-Age Conflict*. Artech House.

Relia, S. (2015). *Cyber Warfare: Its Implications on National Security*. Vij Books India Pvt Ltd.

Rivers, C. (2019). *Russian Cyber Warfare: The History of Russia's State-Sponsored Attacks across the World*. Independently published.

Rosenzweig, P. (2013). *Cyber warfare: How conflicts in cyberspace are challenging America and changing the world*. Praeger.

Sambaluk, N. M. (2020). *Myths and realities of cyber warfare: conflict in the digital realm*. Bloomsbury Publishing USA.

Sambaluk, N. M. (2022). *Weaponizing Cyberspace: Inside Russia's Hostile Activities*. Praeger Security International.

Scott, J. (2017). *Metadata: The Most Potent Weapon in This Cyberwar: the New Cyber-kinetic-meta War*. Createspace Independent Pub.

Springer, P. J. (2017). *Encyclopedia of cyber warfare*. Bloomsbury Publishing USA.

Springer, P. J. (2020). *Cyber warfare: A documentary and reference guide*. Bloomsbury Publishing USA.

Stoddart, K. (2022). *Cyberwarfare: Threats to Critical Infrastructure*. Springer Nature.

U.S. Department of Defense, Strategic Studies Institute, United States Army War College, Department of Homeland Security, Federal Bureau of Investigation. (2017). *International Conflicts in Cyberspace-Battlefield of the 21st Century*. Madison & Adams Press.

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.

Weimer, D. L., & Vining, A. R. (2011). *Policy Analysis: Concepts and Practice*. Longman.

Whyte, C., & Mazanec, B. M. (2023). *Understanding cyber warfare: Politics, policy and strategy*. 2nd ed. Routledge.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security*. Cengage Learning.

Winterfeld, S., & Andress, J. (2013). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Elsevier, Inc.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Broadway Books.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.