Non-Kinetic Warfare and Technological Advancements: An Overview

Aashriti Gautam[*]

Abstract

The paper argues that, in light of the changing warfare dynamics and tactics globally, the concept of non-kinetic warfare has increased the significance of advanced technology in a country's defense sector. Using instances from the ongoing Russia-Ukraine crisis, the chapter further elucidates the emergence of non-kinetic warfare capabilities, particularly cyber warfare, as a new battlefield game-changer. Additionally, drawing

[*] Dr. Aashriti Gautam is an Assistant Professor (Guest) in the Department of Political Science at Shyama Prasad Mukherjee College, University of Delhi. She is a Senior Research Fellow with seven years of academic experience in International Relations at the Center for Russian and Central Asian Studies (CRCAS), Jawaharlal Nehru University (JNU), New Delhi, India. Her research broadly focuses on interdisciplinary studies of conflict, security, and civil-military relations. Her PhD research is in the area of "Russian Nuclear Strategy and its Influence on Foreign Policy, 1993-2018." At a professional level, she has also worked at the Indian Council of World Affairs (ICWA), a prominent think tank under the Ministry of External Affairs dedicated exclusively to studying International Relations and Foreign Affairs. During her tenure at ICWA, she has published two Issue Briefs titled "The Politics of Nord Stream" and "The Greco -Turkish dispute over the Aegean Sea." Her latest article titled "Towards Nuclear Disarmament and Non-Proliferation in Central Asia: Assessment and Prospects for Regional Cooperation" has been published in International Studies - Q2 Journal https://doi.org/10.1177/00208817241228720.

inspiration from the technological progress in cyber warfare on a global scale, it is my argument that India should prioritize the development of non-kinetic warfare capabilities, considering the cyber dangers it encounters due to the China-Pakistan Nexus. In this context, a comprehensive, multifaceted strategy to counter threats posed by low-cost and low-tech to high-cost and specialized technologies is paramount for India. Against this background, the paper has been divided into four sections. The first reviews the existing literature about non-kinetic warfare. The second section examines the growth of non-kinetic warfare capabilities, with a particular focus on cyber warfare as a new battlefield game-changer. This analysis draws upon examples derived from the ongoing Russia-Ukraine issue, specifically highlighting Russia's utilization of cyber and information warfare capabilities against Ukraine. Given the global strides in cyber warfare, the third section focuses on the cyber threats faced by India because of the China-Pakistan Nexus. The final section represents the main conclusions.

Keywords: Non-kinetic warfare, Russia-Ukraine crisis, cyber warfare, China-Pakistan nexus, India.

I. Introduction

The concept of non-kinetic warfare has been extensively discussed in contemporary discourse on warfare, particularly in relation to the ongoing Russia and Ukraine crisis. The term is captivating both in its semantic significance and the ramifications it entails, as it effectively accomplishes the same objectives normally associated with warfare without relying on conventional engagement methods. To provide a more comprehensive analysis, it is imperative to establish clear definitions and distinctions between the concepts of "Kinetic" and "Non-Kinetic." Kinetic actions refer to acts that are executed using physical and material methods, such as bombs, bullets, rockets, and other forms of weaponry. Non-kinetic actions encompass "intellectual, electromagnetic, or behavioral strategies, such as conducting a computer network attack against an adversary's system or implementing a psychological operation against enemy forces. Although non-kinetic acts possess a physical aspect, their impact primarily manifests in indirect ways, such as functional, systemic, psychological, or behavioral repercussions."[1]

The essay entitled "The Changing Face of War: Into the Fourth Generation (1989)" by William S. Lind[2] and his

[1] Teo Cheng Hang. "Non-kinetic warfare: The reality and the response." *Pointer: Journal of the Singapore Armed Forces* 36, no. 2 (2010).

[2] William S. Lind, Keith Nightengale, John F. Schmitt, Joseph W. Sutton, and Gary I. Wilson. "The changing face of war: Into the fourth generation." *Marine Corps Gazette*, (October 1989): 22-26.

colleagues presents a classification of the evolution of warfare into four distinct generations. The ***first-generation warfare (1GW)*** encompassed the methods and strategies employed in warfare during the period leading up to and specifically aligning with the conclusion of the "Peace of Westphalia"[3] in 1648. It was characterized by the deployment of large armies organized in formations known as Lines and Columns on the battlefield. The Cavalry units were also an integral component, wherein the outcome of engagements was mostly contingent upon the numerical strength of the opposing forces. Subsequently, advancements in technology but a lack of innovation in tactics defined ***second-generation warfare (2GW)***. The tactical approach employed in the operation consisted of a combination of linear fire and movement, complemented by the utilization of indirect artillery fire. The emergence of the maneuver approach marked the landscape of ***third-generation warfare (3GW)***. Aerial combat became a significant component. The objective of this tactic was – *first*, to infiltrate hostile territory, bypass their defensive structures, and destroy their communication networks and logistical operations while reducing direct encounters and engagements with enemy force; and *second*, to disrupt the adversary's system of forces using psychological dislocation. The German Blitzkrieg, often known as "Lightning Warfare," during

[3] *Peace of Westphalia, 1648*, ended the Eighty Years' War between Spain and the Dutch and the German phase of the Thirty Years' War. The peace was negotiated, from 1644, in the Westphalian towns of Münster and Osnabrück.

World War II effectively exemplified the principles of the third generation of warfare (3GW). ***Fourth-generation warfare (4GW)*** emerged in the pre-Cold War era when global powers sought to maintain control over their colonies and conquered territories. The Non-State Actors (NSAs) (such as insurgents and militants) who opposed colonial powers faced significant difficulties in matching the state's military capabilities. Consequently, they employed a range of tactics across three distinct dimensions: the *physical dimension* encompasses actual combat operations, while the *psychological dimension* involves influencing the combatants' motivation to fight and their belief in achieving success. Lastly, the *moral dimension* pertains to the manipulation of cultural norms within the context of the conflict.

The emergence of the Internet in the current digital age has given rise to the onset of ***fifth-generation warfare (5GW), commonly referred to as non-kinetic warfare***. This form of warfare is distinguished by tactics such as social engineering, disinformation campaigns, and the utilization of advanced technologies such as Information Technology and artificial intelligence to initiate cyber-attacks. 5GW primarily revolves around the manipulation of perceptions and information. It encompasses not only military strategies but also cultural and moral dimensions. Further, it involves the manipulation of public perception to shape a distorted vision of the world and political affairs. Additionally, the fifth-generation warfare (5GW) strategically leverages cultural icons and religious sentiments to achieve victory over an adversary. The utilization of various strategies to garner political backing from the general population might be considered a legitimate approach, akin to other techniques employed in military operations, such as the implementation of a troop surge in Iraq. Moreover, the efficacy of the Fifth-Generation battle (5GW) is contingent upon its disparity since it does not necessitate unity in its endeavors. The greater the dispersion of efforts in battle, the more resilient and efficient it becomes. Thus, the distinguishing characteristic of 5GW is its omnipresent battlefield and the utilization of both kinetic and non-kinetic force as opposed to relying solely on military might.

II. Literature Review

Throughout history, adversaries have long been involved in conflicts that do not involve direct military confrontation, a phenomenon widely referred to as non-kinetic warfare in the modern period. The concept is not novel within the realm of security discourse. Allusions to this form of warfare may be discerned in the works of various military strategists and thinkers within the domain of international relations. ***Carol Von Clausewitz,***[4] a prominent Prussian military strategist and theorist,

[4] *Carl Philipp Gottfried (or Gottlieb) von Clausewitz* was a Prussian general and military theorist who stressed the “moral,” in modern terms meaning psychological, and political aspects of waging war. Clausewitz was a realist in many different senses, including realpolitik, and while in some respects a romantic, he also drew heavily on the rationalist ideas of the European

expounds on the dynamic nature of warfare in his renowned publication "*Vom Kriege*"[5] (also known as 'On War'). He contends, "*War is not only a true chameleon because it changes its nature slightly in each concrete case, but it is also, in its overall appearance, about its inherent tendencies, a wondrous trinity. His trinity is composed of : primordial violence, hatred, and enmity, which are to be regarded as a blind natural force; the play of chance and probability, within which the creative spirit is free to roam; and its element of subordination, as an instrument of policy, which makes it subject to pure reason.*"[6] In brief, Clausewitz's formulation of the floating trinity encapsulates a conception of warfare that effectively conveys its inherent unpredictability and complexity.

Enlightenment. Clausewitz stressed the dialectical interaction of diverse factors, noting how unexpected developments unfolding under the "fog of war" (i.e., in the face of incomplete, dubious, and often erroneous information and great fear, doubt, and excitement) call for rapid decisions by alert commanders. He saw history as a vital check on erudite abstractions that did not accord with experience.

[5] *Vom Kriege* is a book on war and military strategy by Prussian general Carl von Clausewitz (1780–1831), written mostly after the Napoleonic wars, between 1816 and 1830, and published posthumously by his wife Marie von Brühl in 1832.It is one of the most important treatises on political-military analysis and strategy ever written, and remains both controversial and influential on strategic thinking.

[6] Carl von Clausewitz. *On War*. M. Howard and P. Paret, ed. New Jersey: Princeton University Press, (1989).

Following Clausewitz’s line of reasoning, ***Sun Tzu***,[7] a Chinese military leader, strategist, and philosopher, in his renowned work “*Sun Tzu Ping Fa*”[8] (also known as “The Art of War”) states, “*And as water has no constant form, there are in war no constant conditions*.”[9] The assertion is imbued with a confluence of poetic metaphors, strategically employed to accentuate the intricate nature of warfare. According to Sun Tzu, there exist only five distinct musical notes, yet the sheer abundance of melodies they generate renders it unfeasible to apprehend them in their entirety. In a similar vein, it is worth noting that there exists a total of five fundamental colors, and despite their limited number, the potential combinations they can form are so vast that it becomes impossible to envision them in

[7] *Sun Tzu* was a Chinese military general, strategist, philosopher, and writer who lived during the Eastern Zhou period of 771 to 256 BC. Sun Tzu is traditionally credited as the author of The Art of War, an influential work of military strategy that has affected both Western and East Asian philosophy and military thinking. Sun Tzu is revered in Chinese and East Asian culture as a legendary historical and military figure.

[8] *Sun Tzu Ping Fa* is an ancient Chinese military treatise dating from the Late Spring and Autumn Period (roughly 5th century BC). The work, which is attributed to the ancient Chinese military strategist Sun Tzu (“Master Sun”), is composed of 13 chapters. Each one is devoted to a different set of skills or art related to warfare and how it applies to military strategy and tactics. For almost 1,500 years it was the lead text in an anthology that was formalized as the Seven Military Classics by Emperor Shenzong of Song in 1080. The Art of War remains the most influential strategy text in East Asian warfare and has influenced both East Asian and Western military theory and thinking and has found a variety of applications in a myriad of competitive non-military endeavors across the modern world including espionage, culture, politics, business, and sports.

[9] Tzu Sun. *The Art of War*. J Clavell, ed. New York: Delacorte Press, (1983).

their entirety. Similarly, while examining the realm of battle, it is possible to delineate two distinct classifications of forces: conventional and exceptional. Nevertheless, the vast array of possible combinations that arise from their fusion is limitless, making them inaccessible to the understanding of any solitary human. The two forces under consideration demonstrate a reciprocal process of reproduction, as their connection is continuously sustained, like the interlocking of rings. Who has the power to determine the boundary between the end of one entity and the beginning of another?

Tzu continued: "*To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting…Your aim must be to take All-Under-Heaven intact. Thus, your troops will not wear out and your gains will be complete. This is the art of offensive strategy*."[10] While Sun's notable contribution to the field of warfare mostly focuses on combat strategies, it is evident that he did not perceive kinetic activities as the most optimal path to achieve victory. Sun demonstrated a preference for achieving victory via the utilization of ideas and strategic planning, rather than relying on armed conflict, acts of violence, and the resulting devastation. In the event that kinetic activities were deemed required, it was crucial to ensure that their utilization was limited to the farthest extent possible. According to Tzu, in the pursuit of

[10] Sun. The Art of War.

the ideal, all strategies would seek to attain triumph without engaging in physical conflict. Consequently, any approach that led to combat failed to meet the desired standard. From his perspective, a non-kinetic winning strategy was deemed superior to a kinetic plan.

The concept of non-kinetic warfare also references ***Kautilya***'s *Arthashastra* (Indian manual on the art of politics). According to Kautilya,[11] it is incumbent upon a king to safeguard their subjects from both internal and external perils. To achieve this outcome, the deployment of a military force is deemed necessary. The Mandala Theory,[12] as expounded by Kautilya, includes a discussion on some modern facets of non-Kinetic warfare, which he referred to as Kuta -Yuddha and Tusnim-Yuddha. While Kuta-Yuddha refers to a form of irregular warfare characterized by strategic tactics such as ambushes and raids conducted within the area of the enemy forces, Tusnim-Yuddha on the other hand includes covert operations such

[11] *Kautilya* also known as Chanakya or Vishnu Gupta was an ancient Indian polymath who was active as a teacher, author, strategist, philosopher, economist, jurist, and royal advisor. He authored the ancient Indian political treatise, the Arthashastra, a text dated to roughly between the fourth century BCE and the third century CE. As such, he is considered the pioneer of the field of political science and economics in India, and his work is thought of as an important precursor to classical economics.

[12] *The Mandala system* was a theoretical construction of states by Kautilya in his Arthashastra. The word "mandala" means circle in Sanskrit. It is a geographical concept of division of lands of the king (the vijigishu) and the neighboring kingdoms. It was perhaps the first theoretical work on an ancient system of kings, kingdoms, and empires in the intellectual history of mankind that can be considered to be analogous to a model of international relations.

as sabotage, and targeted killings, and prioritizes cognitive abilities such as intelligence, foresight, psychological acumen, and ingenuity.

The Realist approach, as expounded by Kautilya, is similarly discernible in the works of contemporary neo-realist scholars such as ***Kenneth Neal Waltz and John Joseph Mearsheimer***. They posit that in an anarchic world order, behaviors that are deemed unsavory, such as engaging in warfare, are indispensable instruments of statecraft. Consequently, leaders are obligated to employ these means when they align with the national interest. While both scholars commence their analysis with comparable assumptions, they ultimately arrive at divergent findings. Waltz posits that the attainment of security among nations is accomplished by upholding their relative power in relation to other states. The tendency may result in states demonstrating a steadfast dedication to upholding the existing condition of affairs, therefore aligning with the concept of security maximization. In contrast, Mearsheimer argues that the achievement of national security is dependent on the total eradication of significant opponents. Consequently, to achieve security, countries must strive to achieve global hegemony at the very least or regional domination at the very least without the presence of regional hegemony elsewhere, therefore aligning with the concept of power maximization.[13]

According to Kenneth Waltz's defensive-deterrent theory, the probability of war is substantially diminished when weaponry is developed to impede conquest, dissuade pre-emptive and preventive warfare, and diminish the credibility of coercive threats. The instruments of non-kinetic warfare, such as nuclear deterrence, cyberattacks, information campaigns, and electronic warfare, readily fit within the classification of weapons. As per Mearsheimer, power is the currency of international relations. He posits that in a scenario where all states can inflict harm against one another, there is a strong motivation for them to amass as much strength as they can to deter potential attacks. Mearsheimer argues that the acquisition of power (regional hegemony) necessitates the implementation of certain techniques. First, *War* is the primary method by which power can be acquired, as long as the advantages of engaging in war are greater than the associated drawbacks. Second, *Blackmail* can serve to attain relative gains by coercively pressuring a competitor into accepting concessions. Third, *Bait and Bleed* is when adversaries are deceived into participating in a protracted conflict, enabling the initiating state to accrue relative power from a position of non-engagement. Fourth, the *Act of Balancing* serves to mitigate aggression by dissuading potential aggressors through the establishment of a

[13] J.J. Mearsheimer. *The tragedy of Great Power Politics*. New York: W.W. Norton & Company, (2001).

robust internal military capability or the formation of alliances. Fifth, *Pass the Buck* is the act of passing responsibility to others, which is perceived as more favorable compared to maintaining a balance. In the event of a confrontation, the individual who passes the buck may choose to remain passive while the power dynamics move in their favor. Sixth, *Band wagoning* is a strategic approach that Mearsheimer characterizes as a recourse for entities of significant vulnerability.[14] Therefore, in a nutshell, one can argue that to address uncertainties, potential miscalculations, and future surprises, both Waltz and Mearsheimer advocate the use of military force, incorporating technological advancements as the most efficacious approach to dissuade other countries from infringing upon international peace.

While neorealists explain international patterns and behaviors through "purely material forces, such as military equipment, strategic resources, and financial resources that they see as constituting power."[15] On the contrary, proponents of the ***Constructivist*** perspective contend that the formation of international politics is primarily influenced by ideas rather than tangible entities. The concept encompasses thoughts that are both intersubjective and institutionalized. Constructivists propose an

[14] Peter Toft. "John J. Mearsheimer: An Offensive Realist between Geopolitics and Power." *Journal of International Relations and Development* 8, (2005): 381-408. https://doi.org/10.1057/palgrave.jird.1800065.

[15] Stephen Blank. "Russia's Unending quest for Security," in *The Politics of Security in Modern Russia*, Mark Galeotti, ed. New York: Ashgate Publishing, (2016).

alternative theoretical framework for examining the often-overlooked role of social factors such as prestige and status associated with military capabilities in international relations. From a sociological perspective, they posit that military organizations and their weaponry can be conceptualized as fulfilling functions akin to flags, airlines, and Olympic teams. These entities are perceived by modern states as necessary components for establishing legitimacy and modernity.[16] Further, the constructivists also believe that a country's normative disposition towards military capabilities is also rooted in its society's identity. The concept of identity as it pertains to the foreign policy decisions of a state reflects its position - competitive or accommodating, reclusive or inclusive, high, or low - in relation to other nations. This comparative identity manifests itself in the form of norms that influence the behavioral patterns guiding decisions related to foreign and nuclear policies.[17]

In brief, Constructivists argue that the analysis of global politics should involve an examination of how the interactions between actors contribute to the creation and maintenance of social structures, whether they are cooperative or conflictual. The

[16] Scott D. Sagan. "Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb." *International Security*21, no. 3 (1996): 54–86. https://doi.org/10.2307/2539273.

[17] Karsten Frey. "Nuclear Weapons as Symbols: The Role of Norms in Nuclear Policy Making." Institut Barcelona d'Estudis Internacionals (IBEI) Working Papers, 2006. http://www.jstor.org/stable/resrep14184.

analysis should also consider how these social structures shape the identities and interests of actors, as well as the significance of their material conditions.[18] The conceptual framework proposed by Alexander Wendt holds significant relevance in the context of non-kinetic warfare, particularly hybrid warfare and its civilian dimensions encompassing strategies like deception and propaganda. Thus, in the realm of non-kinetic warfare, conflicts are not limited to intra-state disputes but can encompass clashes between cultural groupings that extend beyond national boundaries and involve various organizations and individuals. In contrast to traditional forms of combat, non-kinetic warfare does not seek to undermine the integrity of a nation-state, nor does it intend to disrupt global peace and stability. In contrast, it exhibits a network-centric approach, instigating conflicts within communities and facilitating a transition from nationalist loyalty towards the state. This manifestation of warfare encompasses a combination of conventional and unconventional strategies, including guerrilla warfare, insurgency, and acts of terrorism.[19]

Additionally, the modern thinkers who are linked with the concept of Fifth Generation Warfare (5GW) include Daniel H. Abbott, Adam Herring, Mark Safranski, Purples Slog, and Curtis G. Weeks. Slog defines 5GW as, “the secret deliberative

[18] Alexander Wendt. “Constructing International Politics.” *International Security* 20, no. 1 (1995): 71–81. https://doi.org/10.2307/2539217.

[19] Asmaa Patel. “Fifth-Generation Warfare and the Definitions of Peace.” *The Journal of Intelligence, Conflict, and Warfare* 2, no. 2 (2019): 15-28. https://doi.org/10.21810/jicw.v2i2.1061.

manipulation of actors, networks, institutions, states or any [0GW, 1GW] 2GW/3GW/4GW forces to achieve a goal or set of goals across a combination of socioeconomic and political domains while attempting to avoid or minimize the retaliatory offensive or defensive actions/reactions of 2GW, 3GW, 4GW powered actors, networks, institutions, and/ or states."[20] Thus, in a nutshell, the concept of 5th Generation Warfare (5GW) also known as non-kinetic warfare revolves around the strategic engagement of perceptions and information. In 5GW, the utilization of violence is executed in an exceedingly covert manner, to the extent that the targeted entity remains oblivious to its status as a victim of warfare. The inherent clandestine nature of this form of warfare renders it the most perilous iteration in the annals of warfare. This warfare hides in the background, and "the most successful [fifth generation] wars are wars that are never identified."[21]

III. Cyber Warfare: A Case of Russia-Ukraine Crisis

Since the advent of the 1990s, advocates of cyber warfare have touted it as a transformative phenomenon within the realm of military affairs, often describing it as the perfect instrument of conflict. In the domain of cyber warfare, three distinct Western schools of thought have been identified. First, *Cyber capabilities and wartime strategy* – it states that the discourse around strategic

[20] Daniel H. Abbot. The Handbook of Fifth-generation (5GW): A fifth generation of war. Ann Arbor, MI: Nimble Books, 2010.

[21] Abbot, The Handbook of Fifth-generation (5GW).

cyber warfare in the 1990s saw it as an emerging battleground with the potential to pose a significant threat to contemporary society. One of the conceptual frameworks that influenced the analysis was the metaphorical concept of a "Cyber Pearl Harbor." This metaphor suggests that with targeted cyber-attacks, it would be possible to disrupt the electrical grid, cause significant damage to essential infrastructure, and effectively paralyze entire economies, all without the reliance on conventional military tactics. Second, *Cyber capabilities on the battlefield* - since the mid-2000s, cyber warfare has been regarded as an ancillary capability that augments traditional capabilities. The strategic usage of cyber operations in a collaborative and coordinated fashion served as a catalyst and amplifier for traditional capabilities. Research indicates that military gear possesses numerous weaknesses that can potentially be exploited through cyber operations. However, in practical terms, the operationalization of such flaws poses significant challenges. For instance, "conventional attacks and disruptive cyber operations, have distinct planning times and operational tempos, making it difficult to achieve joint effects. Malware, for instance, has lifecycles: It must first be developed, tested, and deployed against adversary IT to produce effects until it is discovered and neutralized."[22] Third, *Cyber capabilities between peace and war*.

[22] Matthias Schulze and Mika Kerttunen. "Cyber Operations in Russia's War against Ukraine: Uses, limitations, and lessons learned so far," *SWF Working Paper*, No. 23 (April 2023). https://doi.org/10.18449/2023C23

Since 2014, there has been a significant focus on the hybrid or grey zone characteristics of cyber capabilities. In this perspective, cyber activity is not viewed as a belligerent force in warfare, but rather as an intellectual rivalry wherein the central objective is not to incapacitate military forces but to undermine, capitalize on, and influence the cyber and information landscape.

This concept of hybrid warfare is further exemplified by Russia's military operations in Ukraine in 2014 which showcased several characteristics viz. – political subversion, proxy sanctuary, intrusion, coercive deterrence and negotiated violence. The post-annexation phase was also marked by a prolonged series of cyber assaults against critical Ukrainian infrastructure, orchestrated by organizations with ties to Russia. In November 2015, the Ukrainian electricity infrastructure was subjected to a cyber-attack, leading to a power outage that affected around 230,000 consumers located in Western Ukraine.[23] It was succeeded by the Not Petya ransomware attack of 2017, where the total cost of the attack was estimated at nearly $10 billion globally.[24]

The ongoing Russia-Ukraine crisis, which began on February 24, 2022, is the fourth instance of the Kremlin

[23] "Cyber-Attacks during the Russian Invasion of Ukraine." Office for Budget Responsibility, July 7, 2022. https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/#:~:text=The%20successful%20attack%20in%202015,cyber%2Dattack%20in%20history%E2%80%9D.

[24] "Cyber-Attacks during the Russian Invasion of Ukraine. "

employing military intervention against a bordering country in the period following the Cold War. Furthermore, this incident represents the eighth occurrence in which Moscow has utilized cyber operations, either as a component of a larger campaign or as a standalone means of exerting pressure on a nearby nation.[25] The precise tally of operations conducted during the Russia-Ukraine conflict remains uncertain. However, in August 2022, the Computer Emergency Response Team of Ukraine (CERT-UA) documented 1,123 cyberattacks during the initial six-month period of the war.[26] Another report released by CERT-UA in January 2023, indicated that it has addressed a total of 2,194 attacks.[27] The first pivotal onslaught occurred approximately one hour before the commencement of Russian troop incursion wherein the Viasat satellite communications network experienced disruption as a result of actions undertaken by Russian military intelligence. As to Viasat's official statement, "targeted denial of service attack was initiated by the Russian hackers [that] made it difficult for many modems to remain online... It also executed a ground-based network intrusion… to gain remote access to the trusted management segment of the

[25] Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. "Cyber Operations during the Russo-Ukrainian: From Strange Patterns to Alternative Futures." CSIS, July 13, 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

[26] Schulze and Kerttunen. "Cyber Operations in Russia's war against Ukraine."

[27] Schulze and Kerttunen." Cyber Operations in Russia's war against Ukraine."

network. There, the network issued destructive commands to many residential modems simultaneously."[28]

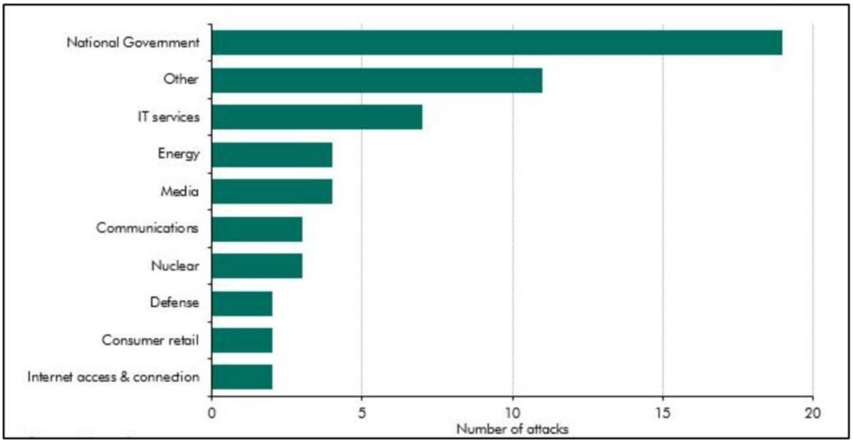


Figure 1: Sector-wise analysis of Cyber-attacks on Ukraine by Russia from February 2022-July 2022.
Source: Office for Budget Responsibility: Fiscal Risk and Sustainability 2022, https://obr.uk/docs/dlm_uploads/Fiscal_risks_and_sustainability_2022-1.pdf.

To gain a deeper comprehension of the cyber dimensions of Russia's military intervention in Ukraine in 2022, it is imperative to consider the distinct way Moscow perceives cyber operations and strategically assesses achievements or setbacks inside the cyber realm. First, the term "cyber," which is commonly used in

[28] Lawrence Freedman. "Russia and the New Language of War." New Statesman, March 14, 2023. https://www.newstatesman.com/world/europe/ukraine/2023/03/russia-new-language-war-cyber-attack.

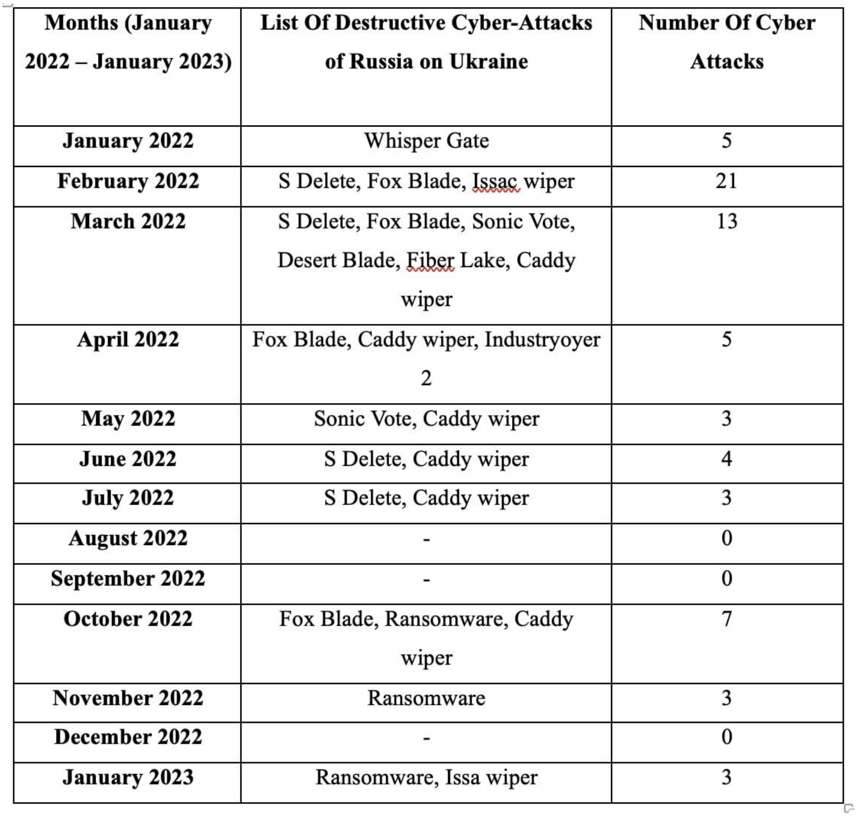
the United States and the West to emphasize the technical integrity of networks, is not commonly seen in the official Russian strategic and military terminology. In contrast, Moscow employs the term "information warfare" to encompass a spectrum of activities, encompassing both technical and psychological aspects, involving the manipulation of code and content, which can be utilized against opposing systems and decision-making processes. Second, in relation to information warfare, it can be observed that Russian strategic culture does not adhere to the conceptual distinctions commonly made by Westerners between peacetime and conflict. The Ukraine incursion serves as an example of how the demands for velocity, influence, and authority in the realm of cyberspace significantly escalate during times of traditional warfare. In such circumstances, the developments occurring on the physical battleground, dictate the tactical and operational necessities. Put differently, cyber forces that are designed for continuous conflict are likely to be deficient in the ability to rapidly increase their capability during times of war.[29] Nevertheless, notwithstanding the inherent constraints, the 2023 Annual Threat Assessment issued by The Office of the Director of National Intelligence articulates "…Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities" and that, "…Russia is particularly focused on

[29] G Wilde. Cyber Operations in Ukraine: Russia's unmet expectations, December 12, 2022. https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.

improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."[30]

[30] "Russia Cyber Threat Overview and Advisories: CISA." Cybersecurity and Infrastructure Security Agency CISA, 2023. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia.

Table 1: List of Destructive attacks of Russia on Ukraine from January 2022 – January 2023



Months (January 2022 – January 2023)	List Of Destructive Cyber-Attacks of Russia on Ukraine	Number Of Cyber Attacks
January 2022	Whisper Gate	5
February 2022	S Delete, Fox Blade, Issac wiper	21
March 2022	S Delete, Fox Blade, Sonic Vote, Desert Blade, Fiber Lake, Caddy wiper	13
April 2022	Fox Blade, Caddy wiper, Industryoyer 2	5
May 2022	Sonic Vote, Caddy wiper	3
June 2022	S Delete, Caddy wiper	4
July 2022	S Delete, Caddy wiper	3
August 2022	-	0
September 2022	-	0
October 2022	Fox Blade, Ransomware, Caddy wiper	7
November 2022	Ransomware	3
December 2022	-	0
January 2023	Ransomware, Issa wiper	3

Source: Microsoft Threat Intelligence Report – A Year of Russian Hybrid Warfare in Ukraine. https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

IV. The Case of India

Russia's Special Military Operation in Ukraine since 2022 has played a crucial role in the examination and implementation of modern ideas about cyber security. The exact consequences of cyberattacks remain uncertain. Nevertheless, it is crucial for Indian officials to carefully monitor the course of the conflict to obtain substantial insights. According to the 2022 report titled "*Cyberthreats to Financial Organisations*" [31] published by Kaspersky, a Russian cybersecurity company, India is positioned within the upper echelon of countries targeted for cyberattacks in the Asia-Pacific (APAC) region, specifically about security breaches that encompass cyber espionage. India is particularly susceptible to Advanced Persistent Threats (APTs), which are highly sophisticated cyber-attacks that exploit vulnerabilities in cybersecurity defenses and remain undiscovered for a prolonged period.[32] According to another recent analysis, it was observed that in the initial quarter of 2023, the average weekly cyber-attacks in India witnessed an increase of 18 per cent when compared to the equivalent time in 2022. Furthermore, it was found that each organization encountered an average of 2,108

[31] "Cyber-Attacks during the Russian Invasion of Ukraine."

[32] Business Standard. "Kaspersky Predicts Rise in Cyber Espionage for India in 2022." January 14, 2022. https://www.business-standard.com/article/economy-policy/kaspersky-predicts-rise-in-cyber-espionage-for-india-in-2022-122011401057_1.html.

weekly attacks during this period.[33] As per the report, Cybercriminals are employing tools such as ChatGPT to generate code, enabling less proficient threat actors to easily initiate cyberattacks. They are also engaging in supply chain attacks by Trojanizing the 3CXDesktop application, all to achieve harmful objectives. According to the Minister of State for Electronics and Information and Technology, Rajeev Chandrasekhar, India experienced a total of 13.91 lakh cyber security incidents in the year 2022.[34] Nevertheless, there was a notable reduction in the frequency of reported cyberattacks in 2022, as seen by a decrease from 1.402 million incidents in 2021. Based on the official statistical data provided by the government, the number of reported occurrences in 2018 amounted to 208,000, whilst the documented attacks reached a total of 394,000 during the same year. In addition, it is worth noting that the Indian Computer Emergency Response Team (CERT-In) was notified of a total of 1,158,000 cybersecurity incidents during the calendar year 2020.[35] The majority of these attacks emanate from Pakistan and

[33] Economic Times. “India Records 18% surge in weekly cyber-attacks in Jan-Mar 2023: Checkpoint.” May 6, 2023. https://cio.economictimes.indiatimes.com/news/digital-security/india-records-18-surge-in-weekly-cyber-attacks-in-jan-mar-2023-check-point/100026695.

[34] Chetan Thathoo. “India Witnessed 13.9 Lakh Cybersecurity Incidents in 2022: Govt.” Inc42 Media, February 13, 2023. https://inc42.com/buzz/india-witnessed-13-9-lakh-cybersecurity-incidents-in-2022-govt/.

[35] Thathoo. “India Witnessed 13.9 Lakh Cybersecurity Incidents in 2022: Govt.”

China, with a specific emphasis on infiltrating the systems that are being targeted.

Following the Galwan skirmish[36] (May 5, 2020 – January 20, 2021) along the Indo-China border, India has emerged as a recurrent subject of cyber offensives allegedly instigated by its unfriendly neighboring nation. Some recent instances of cyber-attacks purportedly linked to China, which have specifically targeted the critical infrastructure of India include – *first,* according to a report issued in 2021 by Recorded Future,[37] a cybersecurity firm based in the United States, it was discovered that the database of the Unique Identification Authority of India (UIDAI) experienced breaches by Chinese hacking collectives during June and July in the same year. The investigation unveiled that the security breaches were manipulated using the malware Winnti, a tool commonly employed by Chinese Advanced

[36] Beginning on May 5, 2020, Chinese and Indian troops engaged in aggressive face-offs, and skirmishes at locations along the Sino-Indian border, including near the disputed Pangong Lake in Ladakh and the Tibet Autonomous Region, and near the border between Sikkim and the Tibet Autonomous Region. In late May, Chinese forces objected to Indian road construction in the Galwan river valley. According to Indian sources, melee fighting on 15–June 16, 2020, resulted in the deaths of Chinese and Indian soldiers. On September 7, for the first time in 45 years, shots were fired along the LAC, with both sides blaming each other for the firing. Partial disengagement from Galwan, Hot Springs, and Gogra occurred in June–July 2020 while complete disengagement from Pangong Lake north and south bank took place in February 2021.

[37] "Major Events and Trends in Cybersecurity in 2022." Manohar Parrikar Institute for Defense Studies and Analyses, 2022. https://idsa.in/system/files/ICCOE_Report_2022.pdf.

Persistent Threat (APT) groups, typically associated with state-sponsored attackers. *Second,* as per another report published by Recorded Future, Chinese hackers used the trojan Shadow Pad and directed their efforts at seven Indian centers located in Ladakh in April 2022. These centers were responsible for executing electrical dispatch and grid control operations near the border region between the two nuclear-armed neighboring countries. *Third,* in December 2022, the All-India Institute of Medical Sciences (AIIMS) in Delhi reportedly experienced a suspected cyberattack, resulting in unauthorized access and potential compromise of personal health data belonging to a substantial cohort of patients. Notably, the attack specifically targeted the sensitive data of prominent individuals, including politicians and celebrities.

Thus, the proliferation of cyber threats within India's digital environment is predominantly marked by a significant volume of infiltrating attacks originating from both Pakistan and China. Furthermore, in recent years, there has been a discernible increase in the degree of collaboration between Beijing and Islamabad in the field of information technology. The incorporation of digital and cyber collaboration holds great significance in the context of the "Long-Term Plan for China-Pakistan Economic Corridor (2017-2030)." This plan places considerable emphasis on the advancement of information and communication technology (ICT)-)-enabled strategies and the facilitation of electronic commerce in Pakistan.[38] This growing China-Pakistan nexus in digital space poses a potential obstacle to the functioning of the Indian democratic system.

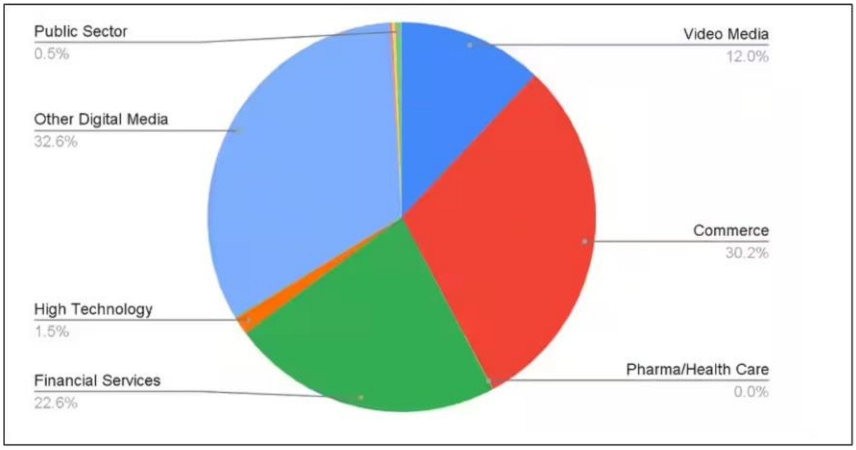


Figure 2: India's total Cyber-attacks by Vertical (between December 2021 and February 2022).

Source : https://www.moneycontrol.com/news/business/193510152-cyber-attacks-on-apis-in-india-between-december-21-and-april-22-akamai-8746771.html

In response to the escalating cyber threats emanating from China and Pakistan, India has implemented the subsequent measures. *First*, the Chief of the Indian Army, General Manoj

[38] Aditya Bhan and Sameer Patil. "Cyber Attacks: Pakistan Emerges as China's Proxy against India." ORF, February 15, 2022. https://www.orfonline.org/research/pakistan-emerges-as-chinas-proxy-against-india/.

Pande, during the Army Commanders Conference conducted in April 2023, declared the implementation of *Command Cyber Operations and Support Wings (CCOSW)* across the Indian Army. The major goal of these wings is to augment levels of preparedness and guarantee the safeguarding of communication networks in this field.[39] *Second*, another significant measure towards mitigating cyber dangers involves the implementation of the highly anticipated *Digital Personal Data Protection Act 2023*, which aims to establish safeguards for the security of personal data and the preservation of persons' privacy. The legislation seeks to enhance the accountability and transparency of various entities, such as internet corporations, mobile applications, and businesses, about the collecting, storage, and processing of individuals' data, in alignment with the principles of the 'Right to Privacy." Furthermore, the act suggests the creation of the *Data Protection Board of India*, which would be responsible for overseeing compliance, imposing penalties, instructing data fiduciaries to implement appropriate actions in the event of a data breach, and addressing concerns raised by individuals harmed by such violations. *Third*, the proposed *National Cyber Security Strategy of 2020* aims to establish a distinct legislative framework for cyberspace and the establishment of a central authority to effectively handle cyber threats, reactions, and complaints. The

[39] Hindustan Times. "Indian Army Raising New Units to Counter China, PAK in Cyber Warfare: Report." April 27, 2023. https://www.hindustantimes.com/india-news/indian-army-raising-new-units-to-counter-china-pakistan-in-cyber-warfare-reports-101682581848934.html.

objective is to establish a complete framework wherein both state-owned and private enterprises are required to adhere to cybersecurity protocols. *Additional steps* have been implemented, such as the establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC)[40] and the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre),[41] to safeguard the nation's important information infrastructure.

V. Conclusion

In light of the above arguments, it is reasonable to conclude that considering the cyber threats faced by India because of the expanding China-Pakistan Nexus, New Delhi should give precedence to the enhancement of non-kinetic warfare capabilities,

[40] National Critical Information Infrastructure Protection Centre (NCIIPC) is an organization of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on January 16, 2014, based in New Delhi, India. It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection.

[41] The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. It is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco system in the country. This center operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. This center is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.

particularly in the realm of cyber warfare. In this context, the policy framework must operate on two distinct levels. *At the national level,* the implementation of a comprehensive National Cyber Security Strategy should be undertaken to safeguard India’s cyberspace, ensuring its security, resilience, and adaptability. Within the present framework, the recently implemented Digital Personal Data Protection Act of 2023 has the potential to initiate a significant transformation in India’s data privacy landscape. Nevertheless, the implementation of this policy has faced scrutiny from members of the opposing party as well as various human rights organizations due to concerns regarding the extent of the exclusions provided.

At the international level, a unified cyber response among nations will bolster security protocols and serve as a strategy to counterbalance China’s dominant presence in the digital domain. In this regard, the G20 Cyber Security Exercise and Drill, conducted during India's G20 presidency to promote collaborative endeavors in strengthening collective resilience against cyber-attacks serves as an exemplary initiative. Thus, in brief, one can contend that the adoption of a comprehensive International Cooperation Framework holds significant implications for India and other nations globally, as it facilitates the efficient reduction of various cyber threats originating from hostile states, which directly affect national security.

Bibliography

Abbot, Daniel H. The handbook of Fifth-generation (5GW): A fifth generation of war. Ann Arbor, MI: Nimble Books, (2010).

Bhan, Aditya, and Sameer Patil. “Cyber Attacks: Pakistan Emerges as China’s Proxy against India.” ORF, February 15, 2022. https://www.orfonline.org/research/pakistan-emerges-as-chinas-proxy-against-india/.

Blank, Stephen. “Russia’s Unending quest for Security.” In *The Politics of Security in Modern Russia*, Mark Galeotti, ed. New York: Ashgate Publishing, (2016).

Business Standard. “Kaspersky Predicts Rise in Cyber Espionage for India in 2022.” January 14, 2022. https://www.business-standard.com/article/economy-policy/kaspersky-predicts-rise-in-cyber-espionage-for-india-in-2022-122011401057_1.html.

Cybersecurity and Infrastructure Security Agency CISA. “Russia Cyber Threat Overview and Advisories: CISA.” 2023. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia.

Economic Times. “India Records 18% surge in weekly cyber-attacks in Jan-Mar 2023: Checkpoint.” May 6, 2023.

https://cio.economictimes.indiatimes.com/news/digital-security/india-records-18-surge-in-weekly-cyber-attacks-in-jan-mar-2023-check-point/100026695.

Freedman, Lawrence. “Russia and the New Language of War.” New Statesman, March 14, 2023. https://www.newstatesman.com/world/europe/ukraine/2023/03/russia-new-language-war-cyber-attack.

Frey, Karsten. “Nuclear Weapons as Symbols: The Role of Norms in Nuclear Policy Making.” Institut Barcelona d’Estudis Internacionals (IBEI) Working Papers, (2006). http://www.jstor.org/stable/resrep14184.

Hang, Teo Cheng. “Non-kinetic warfare: The reality and the response.” *Pointer: Journal of the Singapore Armed Forces 36*, no. 2 (2010).

Hindustan Times. “Indian Army Raising New Units to Counter China, PAK in Cyber Warfare: Report.” April 27, 2023. https://www.hindustantimes.com/india-news/indian-army-raising-new-units-to-counter-china-pakistan-in-cyber-warfare-reports-101682581848934.html.

Lind, William S., Keith Nightengale, John F. Schmitt, Joseph W. Sutton, and Gary I. Wilson. “The changing face of war: Into the fourth generation.” *Marine Corps Gazette*, (October 1989): 22-26.

Manohar Parrikar Institute for Defence Studies and Analyses. "Major Events and Trends in Cybersecurity in 2022." 2022. https://idsa.in/system/files/ICCOE_Report_2022.pdf.

Mearsheimer, J.J. *The tragedy of great power politics*. New York: W.W. Norton & Company, (2001).

Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. "Cyber Operations during the Russo-Ukrainian: From Strange Patterns to Alternative Futures." CSIS, July 13, 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

Office for Budget Responsibility. "Cyber-Attacks during the Russian Invasion of Ukraine." July 7, 2022. https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/#:~:text=The%20successful%20attack%20in%20 2015,cyber%2Dattack%20in%20history%E2%80%9D.

Patel, Asmaa. "Fifth-Generation Warfare and the Definitions of Peace." *The Journal of Intelligence, Conflict, and Warfare* 2, No. 2 (2019): 15-28. https://doi.org/10.21810/jicw.v2i2.1061.

Sagan, Scott D. "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb." *International Security* 21, No. 3 (1996): 54–86. https://doi.org/10.2307/2539273.

Schulze, Matthias, and Mika Kerttunen. “Cyber Operations in Russia’s war against Ukraine.” S*WP Comments*, No. 23 (April 2023). https://doi.org/10.18449/2023C23.

Sun, Tzu. *The Art of War*. Edited by J Clavell. New York: Delacorte Press, (1983).

Thathoo, Chetan. “India Witnessed 13.9 Lakh Cybersecurity Incidents in 2022: Govt.” Inc42 Media, February 13, 2023. https://inc42.com/buzz/india-witnessed-13-9-lakh-cybersecurity-incidents-in-2022-govt/.

Toft, Peter. “John J. Mearsheimer: An Offensive Realist between Geopolitics and Power.” *Journal of International Relations and Development* 8, (2005): 381-408. https://doi.org/10.1057/palgrave.jird.1800065.

Von Clausewitz, Carl. *On War*. M. Howard and P. Paret, ed. New Jersey: Princeton University Press, (1989).

Wendt, Alexander. “Constructing International Politics.” *International Security* 20, No. 1 (1995): 71–81. https://doi.org/10.2307/2539217.

Wilde, Gavin. “Cyber Operations in Ukraine: Russia’s unmet expectations.” Carnegie Endowment for International Peace, December 12, 2022. https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.