Wah Academia Journal of Social Sciences
Volume 4, Issue 1, Jun 2025, pp. 1120-1133
ISSN – E 2958-8731 P 2958-8723

Sino US cyber warfare and its impact on Ukraine war

Uswa Alam[1]

Abstract

This article will provide insight of the cyber dispute between United States of America and Russia and its influence on the Ukraine. The increasing eminence of cyber warfare as a major tool in International Relations which has reformed the old principles of warfare and defense. This research looks into the emergence of US-Russia cyberspace war and concentrating on Ukraine's impacts by Russian invasion. In this cyber dispute, Ukraine's political stability, security hubs and infrastructure destroyed by the Russian hackers as they have launched cyber missiles. During this warfare, cyber-attacks include the disturbance in the energy system from 2015 to 2016, Notpetya attack 2017 and malware campaigns 2022 which leads to economic losses and substantial sabotage. The affiliation of the US with the Ukraine will also be reviewed in terms of the defensive cyber security measures, bilateral relations and strategic repression. It contributes into the understanding of the unconventional warfare and the evolving nature of warfare in the modern age.

Keywords: Cyber warfare, Escalation, NotPetya Attack, Cyber defense

Introduction

US and Russia cyber warfare has become an emergent feature of the world in the 21st century and the power struggle broadened to the domain of cyberspace rather than traditional warfare. The warfare has broadened the battleground into complicated and largely discreet in the domain of cyberspace. As, in the US and Russia digital conflict after the sea, air, space and land cyberspace appeared as the new domain of the conflict. Cyber warfare is basically one nation attacks on other by using digital means to disturb their infrastructure. It is also considered as a powerful tool. The developed strategies of cyber security deeply rooted in historical rivalries of these nations, which now made through the lens of technological

[1] Department of International Relations, University of Management and Technology, Lahore – Pakistan

advancements. Both states have different cyber strategies that contemplate the National security. In latest years, global power dynamic became noticeable in digital battleground like in United States and Russia which are advanced in technological. The US concentrate on the cyber interference, multilateral coordination and durability. While Russia focuses on unsymmetrical tactics such as propaganda campaigns, state sponsored hacking, cyber surveillance and crucial infrastructure sabotage to strengthen its objectives of geopolitics. Both states acknowledge that superiority in information is a key to get benefits in political, military and economic realm. Cyberspace is a powerful weapon open to destruction with high impact and low cost. The intervention in the election campaigns and ransom ware attacks occur through cyberspace and the consequences were long term and real it affects the economic stability and public trust. These digital battlefields between these nations become fluid and unpredictable. This digital conflict between US and Russia affects the Ukraine security. This cyber warfare played an important role in shaping this warfare's course. In February 2022, the Russia- Ukraine war extended into a large-scale intervention which combined with military assault with cyberattacks, economic manipulation and propaganda campaigns. The Ukraine's case is the assortment of traditional and digital strategies with Russia. It was the biggest warfare of the cyber era (parliament, 2023). Meanwhile, Russia positioning a vast array of the digital operations to destroy the infrastructure of Ukraine and mislead public opinion. As Ukraine was supported by the Western allies.

The United States played a pivotal role in resisting Russian cyber assault and supporting Ukraine and helping to defend it. The United States are persistent and largely defensive towards cyber warfare specifically in the incidents such as the 2016 election campaigns interference and 2017 Notpetya attacks. Washington's participated in the Ukraine's conflict in many ways by giving them military, diplomatic and technological support to defend themselves from the Russian's conventional and cyber-attacks. The United States has made many preemptive measures to enhance the cyber defenses of Ukraine and charge heavy costs on Russia for its harmful acts. US strategies are rooted in to develop reactive and proactive stance to protect its infrastructure. In start it's reactive and then moved towards a more proactive stance in its Cyber security posture. The United States enhanced the digital coordination with the Ukraine after the Russia's Crimea annexation in 2014 which includes the Ukrainians cyber security training, exchanging threat information and helping to safe the crucial infrastructure. In 2016 US presidential election, Russia was blame for cyber invasion and false information campaigns to

undermine their electoral process. Through operations like hunt forward the United States cyber command utilized cyber specialist to detect and disable the Russian malicious software. The US government has invested heavy amount in establishing institutions like Department of Homeland security (DHS), National Security Agency (NSA) and the Cyber security and Infrastructure Security Agency (CISA). Its features are developing cyber security strategies like AI, Block chain technologies and machine learning (ML) to protect from the cyber threats, public – private coordination and threat intelligence sharing. The United States not only adopt the defensive measures to obstruct Russian cyber assault, they also adopt the offensive measures. The role of U.S. in the cyber warfare of the Ukraine was a blend of deterring capabilities, defensive operations, diplomacy and digital alliance.

Russia sees cyberspace as a major threat in modern era. Russia use its history in surveillance and further operations by processing it into cyber ones. Russia's role in the cyber warfare of the Ukraine war is both strategic and aggressive. Russia sees the cyberspace as an offensive opportunity by which military and political objectives can be obtained and its offensive operations are aimed to affect politics, unstable opponent and superiority in the digital spaces. Moscow has made a well cyber apparatus which basically include intelligence agencies of states such as GRU and FSB. They have also built the affiliated hacker groups like the Fancy Bear and Sandworm. These operations were led by the agencies like the GRU (military intelligence) and the FSB sometimes collaborate with non-state hacker groups. Russia made these Main Directorate of the General Staff (GRU) military cyber unit for operation against US allies and its interests (harris, 2024). Many of the operations obtained information from both sectors such as governmental and private sector. In early 2000s Russia made its own cyber existence such as hacking and state sponsored cyber operations. Its Cyber operations exploit social segregation and influence public opinion. Russia controls the western norms and rules of cyber security to encourage sovereignty-based model. Russia has made malware engineering and communication techniques to proof its capabilities and maintain strategic equivalency with US and NATO allies in the cyber warfare. Like in 2015 and 2016, blackout occur in the Ukraine because of the cyberattacks on their power grid which was credited to Russian hackers. In 2022 incursion, Russia expanded its cyberattacks by HermeticWiper and WhisperGate to jam Ukrainian banking system and the government (Labs, 2022). Russia also made many attacks like large scale propaganda campaigns to distract people of Ukraine. Through social media platforms, Russia tried to attack on the Ukraine's government and split the alliances

of it with Western Nations. Russia confronted with many unexpected restrictions during the Ukraine incursion.

Ukraine's purpose in this cyber war is both instructive and notable. Ukraine has been at a fortified position in the cyber warfare between the United States and Russia. Ukraine is taken as a testing place for both states (US and Russia). Ukraine's cyber strength is not only responsive, it also demonstrates an era of painful development from the invasions of Russia since 2014. While this Russia cyber-attack on the power grids of the Ukraine in the 2015 and 2016. It taken as an attack on the Ukraine's national security as it damaged the energy sectors at larger scale. US – Russia cyber conflict effects on the Ukraine economically, politically and socially. In 2017, Ukraine's financial institutions are targeted by the Notpetya malware. Because of these billions of dollars and many larger scale multinational companies destroyed (Greenberg, 2019). After these attacks Ukraine create State Service of Special Communications and Information Protection of Ukraine (SSSCIP) to protect Ukraine on the cyber fronts. Ukraine coordinate with the Google and Microsoft to preserve its data in the cloud system to make sure the survival of its governance. CrowdStrike and Mandiant like Cybersecurity agencies helped the Ukraine to hold up against the ransomware and malware attacks. Possibly, the major participation of Ukraine to the domain of cyber warfare is to display that strength is not only acquired for the technological dominance, many other factors like coordination and political determination etc.

Review of the Literature

The literature on the cyber conflict has increased promptly in the last two decades because of an increase in cyber operations by the actors which are state or non-state both. The emerging significance of the cyber realm in international politics has generated new challenges to global security. The uprising of the internet has altered the way states engaged, specifically when it comes to national strategic defense and global power. The cyber dispute between U.S. and Russia view as a considerable issue in the world-politics. It includes a series of the cyber intrusion, malign information campaigns that impacted not only the U.S. and Russia but also other states like Ukraine.

Scholars like Lipnicki and Nye had analyzed that how the cyber instruments are used for the expansion of armed forces and political impact not only for spying. Nye

oriented the term "cyberpower" that the internet is battleground through which they gained influence globally. (Rid, 2012) talks that cyber procedures contain destruction and misrepresentation demonstrate how in the traditional warfare cyberspace used. Real life events have shown actions as of those ideas. Like Russia's hackers spread wrong information in 2016 elections to impact the voters (Withers, 2014). Likewise, the SolarWinds attack which showed that how state-sponsored hackers deeply influence cooperate and government networks which make the defense system weaken. Rid noted that these cyber-attacks might not damage physically but they are powerful enough to damage the stability and the democratic system. These events made sure that how cyber-attacks could made impacts on political, security and economy without military and nuclear war.

Ukraine was being one of the major victims of this cyber warfare. Russia has made a new digital attack on Ukraine's system which was very essential to damage it after the Crimea annexation in 2014.Later in 2015 and 2016 large scale blackouts happened because of the two cyber-attacks on the power grid. (Case, 2016). In 2017, Notpetya malware attack not only disturbed the economy of Ukraine also most of the world. These cyber-attacks disrupted the Ukraine's businesses, trust of the public and operations by government. In all this cyber war, Ukraine acts as a cyber buffer state mean as it is stranded between the U.S. and Russia. Ukraine has faced a lot of repeated attacks in this war. These attacks were made to stop Ukraine to moving towards Western Alliances.

To answer this, Ukraine made it cyber defense stronger by working with the West. Ukraine made its partnership with U.S. and NATO. They provide drills, aids, technical resources and funding. Through these partnerships Ukraine's cyber resilience got improve but the critical challenges were still there. As Ukraine has limited resources which make this cyber warfare defense challenging. Researchers such as Kropac (2017) and Tolkachev (2019) talks that Russia made cyber-attacks on the Ukraine to de-escalate it from making alliances with the West, especially with the NATO and United States not only to damage its system.

U.S. cyber support to the Ukraine, lead to mistrust and threatened for Russia. Russia seen it as an aggressive act which made it to do back to back cyber-attacks. This growing cyber tool usage shows that that the states now don't need the physical wars every time they could also attack on the others cyber spaces. In 2001, John Mearsheimer talks that international relations theories should be updated

according to current situation that how internet has changed national power and global politics a lot.

Theoretical framework

The theory of Security dilemma in the international relations tells us that how states made other states feel unsafe when they are trying to protect themselves. Both states the cyber enhancement of each other as a threat to their own security (Jervis, 1978). Due to this competition occur to take more security measures like military actions and it enhance the concern and pressure. When a state made its defense, stronger other states start taking it as a danger or warning even if it is taken as a defensive. This misconception made a cycle that one's step to increase protection looks as aggressive action and, in the result, it leads to the escalation of the war.

This theory is perfect with this ongoing conflict of cyber dispute between US and Russia. When United States buildup it's cyber defense by upgrading its security system and giving out cyber tools to its allies. Russia takes it as threat not as a defensive and shielding step. As it also takes the Ukraine joining in NATO as a threat (Mearsheimer, 2001). So, Russia answers by building up its own cyber security like spreading disinformation and hacking which is an aggressive action. In response to it, U.S also reacts. It's hard to tell that in cyberspace if a country's cyber actions are for attack or to defend itself. This creates the confusion and made them to respond quickly and it enhances the possibilities of conflict.

Russia sees the support of US and NATO'S for Ukraine as an attempt to weaker the Ukraine's position. While the U.S may see it as help for the ally to provide them the economic and military aid and supporting to build the cyber defenses. So, in answer to this, Russia take an aggressive action. Russia did cyber invasion in Ukraine to destroy their infrastructure and also alarm them to far away from the West. These cyber invasions have made large scale effects on Ukraine like they spread misinformation and start doing propaganda battles to create mistrust in the public. It also disrupts the system of elections. Consistently threats from them create mistrust in the citizens and leads it to more inconvenience socially. Attacks on the banks, companies, power grid and transport made a huge impact on its economy and creates turbulence.

In this digital battlefield, Ukraine is taken in the center of it. To make the west alert, Russia did cyber-attack against Ukraine's to weaken the country .Then U.S send Cyber security support and intelligence to help the Ukraine protect itself, Russia take as it as an interference by the U.S. Russia consider it as a threat by the U.S and answered it more aggressively. In this way, countries end up making more threat, tension and mistrust. In this rivalry between US and Russia both states view other state moves as aggressive but view their own as defensive cyber activities like the US help the Ukraine by giving military, economic aid and sharing its cyber tools. From the view of US, it is a support and let down further attacks while Russia take it as a warning or threat mainly because of the interest of Ukraine in NATO which Russia strictly resist. In response to destroy Ukraine's economy and system Russia has used the cyber tools like the 2015 & 2016 Ukraine's power grid cyber-attacks and destruction of billions of dollars and intelligence with Ukraine and Russia views it as a control in that area. Because of this Russia made much more tools and weapons for digital attacks on the Ukraine and Western.

This repeating and going on cycle is exactly describes the security dilemma. Every state thinks that it is just securing its own interests. As they don't believe on each other so they take every action as a possible threat or attack which escalate pressure, anxiety and threat of the conflict (Rid, 2020). Russia made cyber-attacks not only to destroy system of Ukraine but also want to convey a political message to stay away from the US. These attacks have serious impacts politically, socially and economically on the Ukraine. By creating disturbance in elections, they brought mistrust in the government. Socially the citizens' start thinking that the state is unable to protect them which leads to the division meanwhile economically stability decrease and development slows down because of the cyber-attacks in the transport, companies and banks. Ukraine becomes more reliant on the Western support in trying to defend itself such as joining NATO and made its own State Service of Special Communications and Information Protection (SSSCIP). These actions were made to improve the security of the Ukraine but it creates a sense of fear in Russia. Every action added fuel to the fire. Every action for the protection leads us to the disputes and instability.

In this cyber warfare between the two superpowers Unites States and Russia, Ukraine encounters the most destruction. This case shows that every try to enhance the security and protection took it to more war and disruption until the both states don't have some rules to follow and they didn't communicate with each other.

The primary objective of this research is to evaluate the cyber dispute between the United States and Russia, and examine the direct and also the indirect effects on the Ukraine's political stability, security hubs and infrastructure. Furthermore, the study aims to focus on to examine the history, advancement of the U.S. and Russian cyber tactics and how the cyber war between U.S. and Russia has become a digital battlefield for the Ukraine. To explore that in the cyber war between the U.S. and Russia how Ukraine has involved in the cyber battlefield. This research aims to identify the role of UN and NATO in improving its cyber defense measures.

Methodology

The research methodology for this study utilized a qualitative approach through the evaluation of existing data derived from reports, documents and literature belongs to the research study. It is grounded on the report approach, which concentrates on the larger scale cyber strikes faced by Ukraine. Like the cyber strikes on the power grid of Ukraine in 2015 and 2016, Notpetya attack on Malware in 2017 and many other cyber-attacks between the Russia-Ukraine during the 2022. By analyzing these reality-based cases, the article will provide a view that how these cyber strikes impacted on the Ukraine's and this all information gathered from many different sources main and supporting like case reports, literature, interviews, articles, journals and documents.

Discussion

By applying the security dilemma theory, it becomes clear that the cyber conflict in between Russia and the United states has considerably revised the conventional insight of warfare in the international relations.

- **The Notpetya Attack 2017**

A malware model which is known as NotPetya immediately disperse in Ukraine. This Attack firstly on their accounting system and tax which is used by the Ukrainian businesses. This malware is made not for the financial benefits but to destroy all the data and somehow it resembled ransomware. The purpose of this attack was to create economic instability and give punishment to Ukraine for not avoiding West as Russia warned to stay far away from the West. Due to this Ukraine's media channels, government agencies, infrastructure and banks damaged.

❖ **Deterrence and Evolution of warfare in IR**

Not alike traditional military dispute that depends on kinetics force, cyber conflict works in the gray zone- under the boundary of open conflict but able of creating tactical interference. Russia's imputed role in cyber wars such as the NotPetya war (2017) involvement in the (2016) US elections recurring incursions into strategic assets shows how cyber abilities are being used to attain strategic goals without physical encounter.

Likewise, US-led activities and tactics such as the Cyber orders "Defend-Forward" demonstrate foresight oriented at discouraging enemies by continuously involving them in cyber world.

Disincentive, conventionally embedded in the risk of revenge attack has also developed. In cyber world acknowledgement is not easy and the delayed feedbacks, creating conventional restraint models ineffective. In place of denial strategy if defense will be strong it makes war less efficient-and the entanglement deterrence increasing the stakes of cyber war -through financial interdependence have taken on greater relevance. This emerging terrain has effects for judicial frameworks and international relations. The cyber war between these super developed countries has provoked debates in the different forums like NATO and UN about developing guidelines for behavior in cyber world.

So, the conclusion is the US-Russia cyber conflict has converted the conflict from a physical to digital realm -revised the policy making and thinking again about it how dominance is asserted and wars are managed in the digital era.

Cyber Conflict as a strategic instrument in World politics

Research studies of 2017 NotPetya and cyber campaigns 2022 emphasize a crucial reality that cyber conflict is a significant part of advanced level statesmanship. Cyber-attacks allow the states to assert dominance even without entering into the territory of other states like traditional warfare. Through cyber operations, Russia made political issues, disinformation and disturbance strategically in the disputed regions of the Ukraine. In this conflict, US and Russia both effort for the advancement in technology. So, they can get dominance over other. Russia tried to attach on the cyberspace of the Western but on the other side, US keeps a focus on the cyber security to protect its allies.

Role of the Technology

A major factor in the advanced cyber war is the technological domain. Ukraine got the support of the companies likes Google, Cloud system, Microsoft for the defense as it provides the security to the data and protect the infrastructure. Cyber security is essential for the state. If a state doesn't have enough technological power to protect its states then its survival is in danger.

- **Ukraine became the lead unit in the cyberspace**

Ukraine became a strong cyber actor in 2022 as it improves its defense system. Before this, it was at risk in 2014 as it can't defend themselves at that time. In start, Russia cyber-attacks on the Ukraine such as spread disinformation, propaganda campaigns, destroy power grid and malware attacks. But in 2022, Ukraine became a lead unit in the cyber potency. Some major components behind the transformation of Ukraine has the alliance with the companies of private technology, cyber information programs and get support of the international organizations like the US and NATO (CSIS 2022). Ukraine's scenario also gave the idea of how to defend and recover from the cyber invasion.

- **Role of US and NATO**

The international organizations just like the US and the NATO which is North Atlantic Treaty Organization do an emerging yet circumscribed role in regulating and administering the cyber war between these two countries Us and Russia. While these organizations lack inadequate implementation in cyber world, they serve a proper forum for discussion, collective norm development and security strategies.
And particularly the United States through the open-ended working groups and group of government experts has assisted conversations on accountable state conduct in cyber world. These kinds of platforms have formed non-binding standards such as stopping the attacks on core public infrastructure during period of peace. Although these countries Russia and the US get involved in these discussions, their competing interests impede consensus.

And specifically, Russia supports for a state controlled internet model on the other hand The US advocates internet independence and the different stakeholders governance. This deviation hinders the US's regulatory power but supports its role as moderator and organizer.

NATO has assumed a more proactive stance in cyber defense strategies. At the 2016 Warsaw Summit, cyberspace was officially recognized as an operational domain, indicating that a cyber-attack could potentially invoke a collective military response under Article 5. Since this recognition, NATO has concentrated on strengthening cyber defenses, improving intelligence sharing, and participating in joint training exercises, particularly in response to cyber threats emanating from Russia, which target member nations and partners such as Ukraine. The Cyber Defense Center of Excellence in Estonia plays a crucial role in research and coordination within this domain.

Despite neither the US nor NATO having entirely filled the gap in cyberspace, they stay vital in fostering standards, fortifying cooperative defense, and exerting influence for responsibility. Their initiatives, although limited, signify crucial moves toward mitigating digital rivalries between the Western power and the Eastern nation in a largely uncontrolled and volatile sphere.

Conclusion

This research gives us the insight of the effects of U.S. and Russian cyber warfare on the Ukraine and how cyber war has become a major factor of the competition between the states. It highlights the major progress in security studies and International Relations. Especially we come to know about how the Ukraine has been involved in this cyber warfare. Ukraine was playing the role of battlefield for both states. Russia and its actors have mainly impact on the Ukraine's national security and cyber security postures. Like the cyber strikes on power grid of the Ukraine in 2015 and 2016, Petya Malware attack 2017 includes banking system was alarming for the Ukraine's administrations. Russia did large scale intervention in Ukraine which shows the geopolitical imagery of the cyber-attacks. These digital tools are not just tactical tools but also works as the strategic objectives. Russia cyber-attacks on the Ukraine to disturb its election process and political system. Regardless of the ongoing attacks, Ukraine started investing on the cyber defense posture to made it better. This results in the cooperation with the NATO, EU, US and various other western associations who helped Ukraine by the cyber defense training and sharing intelligence. To made its status stronger nationally and internationally, Ukraine has to prioritize the trust and engaging with the people. This research also shows the limited cyber power. Even though Russia made large

attacks on Ukraine but still it failed to get strategic influence or disable the Ukraine's cyber ecosystem.

References

Beska, S. (2023). Cybersecurity and cyber resilience in Ukraine: Challenges and strategies. Central European University.

Case, D. U. (2016). Analysis of the cyber-attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388(1–29), 3.

Giles, K. (2015). Russia and its neighbours: Old attitudes, new capabilities. In K. Geers (Ed.), Cyber war in perspective: Russian aggression against Ukraine (pp. 19–28). NATO CCD COE Publications.

Gjesvik, L. (2022). Cybersecurity and the Ukraine conflict: Implications for European security (NUPI Policy Brief 8/2022). Norwegian Institute of International Affairs.

Gotsiridze, A. (2023). Brief characterization of Russian cyber actors before a full-scale invasion of Ukraine. Scientific and Practical Cyber Security Journal, 1(3), 12–20.

Greenberg, A. (2019). Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Knopf Doubleday Publishing Group.

Harris, S. (2024). Russia's most notorious special forces unit now has its own cyber warfare team. Retrieved from [URL missing].

Huang, Y., Huang, L., & Zhu, Q. (2021). Reinforcement learning for feedback-enabled cyber resilience. arXiv Preprint, arXiv:2107.00783.

Jaitner, M., & Geers, K. (2015). Russian information warfare: Lessons from Ukraine. In K. Geers (Ed.), Cyber war in perspective: Russian aggression against Ukraine (pp. 87–94). NATO CCD COE Publications.

Jasper, S. (2022). Russian cyber operations: Coding the boundaries of conflict. Georgetown University Press.

Jervis, R. (1978). Cooperation under the security dilemma. World Politics, 30(2), 167–214.

Jonsson, O. (2018). Hacks, leaks and disruptions: Russian cyber strategies. Journal of Cyber Policy, 3(1), 53–64.

Kolodii, R. (2024). The pedagogy of cyber-war: Explaining Ukraine's resilience against Russian cyber-aggression. Defense & Security Analysis, 1–22.

Kostyuk, N., & Gartzke, E. (2022). Why cyber dogs have yet to bark loudly in Russia's invasion of Ukraine. Texas National Security Review.

Labs, L. (2022). A technical analysis of HermeticWiper malware: Threat intelligence report. Retrieved from [URL missing].

Lupovici, A. (2021). A methodology for cyber deterrence research. International Studies Review, 23(4), 1672–1698.

Maschmeyer, L. (2024). Cyber conflict and subversion in the Russia-Ukraine war. Lawfare. Retrieved from [URL missing].

Mearsheimer, J. J. (2001). The tragedy of great power politics. W. W. Norton.

Muzayan Haq, M. Y., Abhishta, A., & Sommese, R. (2023). Assessing network operator actions to enhance digital sovereignty and strengthen network resilience: A longitudinal analysis during the Russia-Ukraine conflict. arXiv Preprint, arXiv:2305.17666.

Parliament, E. (2023). Cybersecurity in the EU and Ukraine in the context of Russia's aggression. Brussels: [Publisher not listed].

Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Profile Books.

Sandoval, O. C. (2022). Using cyber threat intelligence to support adversary understanding applied to the Russia-Ukraine conflict. arXiv Preprint, arXiv:2205.03469.

Schneider, J. (2020). The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. In Emerging technologies and international security (pp. 45–60). Routledge.

Shires, J., Kaminska, M., & Smeets, M. W. E. (2022). Cyber operations during the 2022 Russian invasion of Ukraine: Lessons learned (so far). European Cyber Conflict Research Initiative.

Shypovskyi, V. (2023). Enhancing the factor analysis of information risk methodology for assessing cyber-resilience in critical infrastructure information systems. Journal of Cybersecurity and Information Systems, 5(3), 45–58.

Vernygora, V., & Vdovychenko, V. (2023). Ukraine's resilience lessons learnt: Perspectives and challenges ahead of the NATO Vilnius Summit. Scientific Investigations of Current Issues in Private and Public Law, 2023(2), 7–15.

Weber, V. (2022). States and their proxies in cyber operations. Journal of Strategic Studies, 45(6–7), 885–911.

Weber, V. (2022). Using information to influence the Russian war in Ukraine. Journal of Information Warfare, 14(7), 45–60.

Withers, P. (2014). Jason Healey. A fierce domain: Conflict in cyberspace, 1986 to 2012. The Chief of the Air Staff's Reading List, 21–22.

Yeremenko, O., Lemeshko, O., & Yevdokymenko, M. (2019). Cyber resilience approach based on traffic engineering fast reroute with policing. In IEEE International Conference on Advanced Trends in Information Theory (pp. 168–172). IEEE.

Article Information:

Received	5-*Apr*-2025
Revised	28-May-2025
Accepted	10-Jun-2025
Published	15-Jun-2025

Declarations:

Author's Contribution:

- **Conceptualization, and intellectual revisions**
- **Data collection, interpretation, and drafting of manuscript**
- The author agrees to take responsibility for every facet of the work, making sure that any concerns about its integrity or veracity are thoroughly examined and addressed

- **Conflict of Interest**: NIL
- **Funding Sources**: NIL

Correspondence:

Uswa Alam

uswaa@gmail.com