The Paradox of Cyber Warfare and Clausewitz's Conception of War

NUST Journal of International Peace & Stability
2025, Vol. 8(1) Pages 17-29
njips.nust.edu.pk
DOI: http://doi.org/10.37540/njips.v8i1.183

***Nageen Ashraf**[1]

Abstract

The technological advancements of the 21st century have broadened the traditional concepts of warfare and security. This broadened notion of warfare and security contains an important element of cyberspace. Cyberspace is the virtual space created through the linkages of the internet and internet devices. Because of certain developments, cyberspace is now considered the fifth operational domain for warfare, with the other four domains being land, sea, air, and space. This new realm of confrontation has encouraged states worldwide to secure their cyberspaces and build offensive or defensive cyber warfare capabilities as per their potential. Where traditional realists argue that cyber warfare does not fit the concept of warfare (as proposed by Clausewitz), this article justifies otherwise. The study employs content analysis as a method and adopts a qualitative approach to data analysis, posing the following research question: How does cyber warfare fit Clausewitz's conception of war? In exploring this, the research hypothesizes that an in-depth analysis of Clausewitz's trinity—the elements of violence, combat, and policy—indicates that these elements are also the salient features of cyber warfare, making it a *valid* form of war despite its anomalies.

Keywords
Cyber warfare, cyber security, national security, Clausewitz's trinity

Introduction

The 21st century is widely regarded for its digitalization and technological advancements, and because of this, the global use of the internet has also been upsurging. With the growth of the global population and increasing integration, the number of internet users worldwide has also risen significantly. Data shows that internet users in the past decade increased from 1.97 billion in 2010 to almost 4.5 billion in 2020 (Kemp, 2020). On the one hand, the internet has now made access to multiple

[1] *****Corresponding Author: *Nageen Ashraf* is an Assistant Research Associate (ARA) at the Islamabad Policy Research Institute (IPRI), Islamabad, Pakistan
E-mail: nageen.ashraf@ipripak.org

Received 14 February 2023; **Revised** 16 September 2024; **Accepted** 22 January 2025; **Published online** 31 January 2025

sources and parts of the world more accessible than ever before. On the other hand, it has come with repercussions because the more dependent the world is on the internet, the more vulnerable it will become to cyber-attacks and hacks.

As these advancements have unfolded globally, warfare and security have also evolved. Undoubtedly, cyberspace has reduced the barriers between states and given them a platform to stay connected and increase their diplomatic ties. However, cyberspace has opened the world to a new coliseum of confrontation and conflict. By redefining the nature of warfare and security, the internet and cyberspace have raised multiple security concerns for the states on a global level. Previously, wars were fought between states on the battlefields involving kinetic elements, but there has been a paradigm shift from a physical to a virtual mode of war. It is a mode of warfare that does not require physically trained warriors or battle-field experts; instead, cyber warriors can now put a state's national security at stake.

This research paper attempts to deeply explore the notion of cyber warfare through the lens of Clausewitz's trinity of war. It considers secondary sources of data, including books, journal articles, newspaper articles, and other literature on cyber warfare, to determine if cyber warfare fits the traditional notion of *war* opined by Clausewitz. In exploring this primary research question, the research considers the famous trinity of war composed of violence, combat, and policy to justify whether cyber warfare is a *valid* or *true* form. The research applies content analysis as an instrument and opts for qualitative data analysis. In applying the trinity of war to cyber warfare, the research also highlights the notions of uncertainty and friction when it comes to combat in cyber warfare. The research is significant because it contributes to the existing literature on cyber warfare, hypothesizing that although traditional definitions of war have some limitations, the in-depth analysis of Clausewitz's definition of war portrays that cyber warfare is a valid form of warfare despite its anomalies concerning traditional warfare.

Cyber Warfare

Cyber warfare is a branch of hybrid warfare that necessitates cyberspace to disrupt the enemy's critical infrastructure. Here, cyberspace is the virtual world of computers. Where traditionally, the concept of 'space' was confined to geography and territoriality, cyberspace is gradually ceasing the existence of this concept (Choucri, 2012). The notion of cyberspace is the location or virtual space that is created because of the linkage between computers on a global level (Bussell, 2013). Cyberspace is "a time-dependent set of interconnected information systems and the human users that interact with these systems" (Fang, 2018, p.3). Unlike the physical space around us, including the land, oceans, and air, cyberspace cannot be demarcated and divided into national boundaries. Sharma (2011) suggests that cyberspace falls under a subcategory of communication systems and is the same as information or communication space.

The Internet is an important component in cyber warfare because it acts as a platform that connects all electronic devices; however, technological advancements have blurred the line between the Internet and cyberspace. (Cepik et al., 2015). Even though there is no universally accepted definition of cyber warfare, and it varies from state to state and scholar to scholar, this paper highlights some important definitions of cyber warfare taken from different sources to point out how each idea differs from the other as elaborated below:

- There has been little consensus on the definition provided by Clarke and Knake (2010, p. 292) in their book *'Cyber War: The Next Threat to National Security and*

What to Do About It.' According to the definition, cyber war refers to the "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." This definition generally explains the concept but lacks clarification on the involvement of non-state actors, one of the significant features that make cyber warfare distinct from previous warfare (Abdyraeva, 2020).

- According to Billo and Chang (2004), cyber warfare involves offensive and defensive cyber operations in which different units are organized outside nation-state boundaries and use electronic means to attack other networks or computers.
- Under the U.S. National Research Council's Committee on Offensive Information Warfare, cyber warfare precludes cyber-attacks that aim to gather information. On the other hand, the U.S. Department of Defense includes information-gathering cyber-attacks as part of cyber warfare (Bell, 2018).
- Similarly, one of the widely used definitions of cyber warfare is given by Jinghua (2019), who equates cyber warfare to strategic warfare in the 21st century, similar to nuclear warfare in the 20th century. This idea bestows significant importance on cyber warfare and certifies that it is an important national security concern.
- In addition, Goel (2020) incorporates international organizations into the cyber warfare realm and defines cyber warfare as "a broad term that refers to actions by nation-state actors (or other international organizations with mala fide intentions) to use hacking tools to achieve military objectives in another country" (Goel, 2020, p. 89).

Where scholars have argued that hybrid warfare is not a new concept, the elements of cyber warfare are also not entirely new. Undoubtedly, technological advancements have given rise to cyber warfare. However, the important components of cyber warfare, i.e., sabotage, espionage, and subversion, have always been a part of the conflict, even before the technological developments. The only difference cyberspace made is that of a non-violent element. Previously, espionage, subversion, and sabotage could not have been carried out without violent force or physical damage, but cyber warfare has made it possible (Rid, 2011). Likewise, it is not the first-time states have attacked adversaries' critical infrastructure. The strategy is as old as it was implemented in World War II when the U.S. aimed at Germany's critical infrastructure through air bombing by targeting their critical infrastructure (Lewis, 2002).

At the same time, cyberspace has brought dramatic changes in the domains of espionage, subversion, and sabotage, and its restrictions are not comparable to the physical element of traditional warfare (Rid, 2011). Nevertheless, as states become increasingly dependent on the internet and technology, they become more vulnerable to cyberterrorism and cyber-attacks (Lewis, 2002). As globalization increases and the world becomes increasingly interconnected, more people and systems are expected to be affected by cyber-attacks (Billo & Chang, 2004).

Peculiarities of Cyber Space.

Cyber warfare is a complex phenomenon because of virtual space and the involvement of multiple actors. It has several anomalies that distinguish it from conventional warfare. Some of these peculiarities give this form of warfare an upper edge in the war-fighting domain and make its execution easier than a physical attack.

Variety of Actors

The Internet is a considerable platform connecting millions and billions of people worldwide, which can be exploited by nation-states or non-state actors, including hackers, criminal groups, terrorist groups, or individuals for different objectives (Hathaway, 2008). Non-state actors now possess technological abilities they did not have access to earlier (Otaiku, 2018). Some sources highlight that terrorist groups tend to update their systems along with the technological advancements and have been seen attacking states that are more dependent on technology; however, some argue that since cyber-attacks are not as impactful as physical attacks in their ability to cause physical destruction, terrorist groups do not give much importance to these attacks (Wilson, 2008).

No Superpower

The territorial, naval, and aerial superiorities of a state make it a superpower in that particular *space*, but that is not the case in cyberspace. No matter how sophisticated a state's critical infrastructure is, its chances of being attacked are always high. As mentioned earlier, the more dependent a state is on the internet, the more exposed it is to cyber-attacks and hackers. Even though the criterion of cyber superpowers is yet to be defined, some scholars argue that the U.S. and China are the two key players in this domain, fighting each other. There is a disagreement between some scholars who regard the U.S. as the cyber superpower and others who regard China's capabilities as stronger. However, it is to be noted that both states are as vulnerable as the other, which makes it challenging to decide which one is a cyber-superpower. Also, states like Israel, Russia, India, North Korea, and even Iran are not far behind and can be regarded as major cyber powers. They are considered to be the states that have cyber warfare capabilities. As Chen (2010) put it, every state has the necessary weapons (software and computers) to fight a cyber war without the state being a superpower.

Cost-Friendly

Cyber-attacks do not need heavy machinery, well-equipped armed forces, and sophisticated missile technology to make an impact on the opponent. These factors defined the victory in traditional wars, but cyberspace has changed the notion. Even though technological sophistication is required for a better defense in cyberspace, that does not necessarily make states less vulnerable to cyber-attacks. The offensive cyber operations do not require a large budget to be carried out compared to the economic costs of a physical battlefield (Hathaway, 2008). Thus, even an individual with a minimal budget but good technological knowledge can put the national security of a state at stake.

Anonymity

The problem of attribution in the cyber domain is an important concern. It is also regarded as one of the factors that facilitate and encourage non-state actors and terrorist groups to launch attacks through electronic means instead of conventional ones. One cannot punish an offender if he is not identifiable (Rid, 2011). If state 'A' carries out a cyber-attack against state 'B,' state 'B' would never know if state 'A' carried out the attack. Even though the systems sometimes attribute the attack to a particular state, the sources disappear when some legal process takes place to hold the attacker state responsible (Tiirmaa-Klaar, 2011). Secondly, even if state A is accused of carrying out that attack, state 'A' can rebuff the accusation and claim that a third party attacked without taking the state into confidence. In this way, an attacker can remain anonymous for as long as it takes, and the attribution problem remains.

No Discrimination in Targets

No warfare is more irregular than cyber warfare, and increasing technological advancements have blurred the line between cyber terrorism and cyber warfare. Cyber-attacks do not always have military objectives; sometimes, they might be directly related to civilians. For instance, cyber-attacks like information theft are directly linked to civilians and can cause insecurity among them (Cavelty, 2014). Also, technological involvement makes the risks associated with cyber-attacks enormous. Because these attacks are executed through technology, their impacts might be uncontrollable because of technological complexities. They may produce unpredictable outcomes, causing damage far more significant than expected. This is also one of the reasons there are fair chances of cyber-attacks escalating to physical destruction (Wu & Huang, 2020).

Offensive Superiority

Classical realists argue that the defensive capabilities of a state should be robust enough to allow it to retaliate in case of an offensive attack. A notable realist, Clausewitz, claims that *defense* is always better than *offense* and is more potent than offensive strategies in terms of waging war (Clausewitz, 2007). This claim, unfortunately, does not apply to cyberspace, where offensive attack already has an advantage over defense (Goldsmith, 2010). Defense is about securing the systems and keeping all the external actors out of them, but that is not possible in cyberspace because there is much unpredictability in cyber-attacks. It might be that state ‘A’ was expecting an information theft by state ‘B,’ but instead, state ‘C’ launched a cyber-attack on state A’s critical infrastructure. Furthermore, to rule out the possibility if we argue that state A secures all its systems to avoid all sorts of cyber-attacks is an impossible thing. No matter how defensive state A’s information systems are, they will always be vulnerable because of the inevitability of cyber-attacks.

The Clausewitz’s Trinity: War as Violence, Combat and Policy

The notion of national security is often considered a combination of ‘nation’ and ‘security.’ This relates national security to the idea of protection, safety, and well-being of the nation, where these factors are common to all (Paleri, 2008). Thus, any attempt that directly or indirectly affects the nationals of a state is considered a threat to the state’s national security. In contemporary times, cyber security is linked with the state’s national security because of its ability to affect decisions, its nationals, and their daily life routines. This very argument also highlights the role of people, government, and the military regarding cyberspace and cyber warfare.

In contemporary times, cyberspace is the easiest and most effective way to disrupt the infrastructure and industries of a state (Poindexter, 2015). War is simply a form of aggression between states. The United Nations General Assembly (UNGA) defines ‘aggression’ as the use of any weapon from one state to another or bombardment from one state to another (Wilson, 2008). Looking at this idea of aggression, cyber warfare does not follow the definition provided by UNGA. This is because the characterization focuses primarily on the nation-states and does not discuss the involvement of non-state actors. Secondly, there is also no consensus about cyber tools regarded as cyber weapons[2], which again restricts cyber warfare to infusing into this definition.

Correspondingly, some scholars question if war in the cyber domain can be considered a *true* form of war because of its inefficiency in fitting into the traditional definition of 'war' proposed by Clausewitz. According to Clausewitz's concept of war, no cyber-attack has ever occurred that could be considered an *act of war* (Hadfield, 2016). So far, the incidents that have taken place in cyberspace have not caused destruction to the threatening level, be it the number of deaths or the attacks on critical infrastructure (Valeriano & Maness, 2015). This raises concern about cyberspace being a battlefield for warfare because of the absence of physical frontlines (Missiroli, 2019). Moreover, critics argue that cyber-attacks so far have not been able to fulfill the given Clausewitz's criteria of war (Rid, 2011).

Clausewitz defines *war* as having three major elements: violence, combat, and policy; these elements correspond to the emotions of people, the chance and friction faced by the military commander, and the rational policy of the government. It can also be regarded as an act of force to compel our enemy to do our will. From the definition, it is evident that the violence (use of force), combat, and political nature (influencing the opponent's will) make a certain act *an act of war*. In order to understand if cyber warfare is a *true* form of warfare, according to Clausewitz, it is important to look at his definition of war from a broader perspective. The research will divide Clausewitz's definition into these three parts to explore each element individually.

War as an Act of Violence

In the first half of Clausewitz's definition, where he talks about the kinetic element (an act of force), it is essential to note that cyber-attacks can cause physical damage to critical infrastructures if targeted. Even though previous cyber-attacks have not been able to escalate to such an extent that they cause severe physical damage, it does not necessarily mean that future cyber-attacks will also lack the kinetic element. For instance, in contrast to all the previously designed cyber-worms[3], Stuxnet[4] was designed to target physical infrastructures specifically. Likewise, it must be taken into account that with all other traditional domains of warfare, cyberspace has been regarded as the fifth operational domain (Abdyraeva, 2020; Ebert, 2020). This signifies that conflict and warfare are inevitable in this new domain, which should be given the same importance regarding security as the other four domains of space, air, land, and sea.

Cyber warfare is inevitable, and the conception that cyber-attacks are not capable of causing as much destruction as 9/11 or Pearl Harbor sets aside the security threat fostered by cyber-attacks. Security experts in the U.S. have emphasized that a well-coordinated cyber-attack can magnify the effects of a conventional attack (Wilson, 2008). It is noteworthy that several cyber-attacks aimed at stealing credit card information among the USA's citizens have been used to financially support terrorist

[2] A cyber weapon is any code-based instrument that relies exclusively on digital networks. It can damage their integrity or penetrate them to gather sensitive information that would be advantageous in a kinetic attack.

[3] Worm is a program replicating itself like a virus to spread to different computers via a computer network. It does not attach itself to any program or file.

[4] The U.S. and Israel designed a cyber weapon, Stuxnet, to sabotage the Iranian nuclear program by targeting ICSs (Industrial Control Systems). Stuxnet showed a level of sophistication not previously seen in malware. The Stuxnet worm was a complex malware program that could stealthily move from system to system, replicating itself and effectively reprograming critical systems while hiding the modified code from human controllers.

groups that have conventional capabilities (Wilson, 2008). In this way, the cyber-attacks contribute to financing actors that are a serious (indirect) threat to the state's national security.

It is also argued that a cyber-attack can be as fierce as a nuclear attack; cyber-attacks on critical infrastructure can also affect the states' national security. The world has already seen the episode of 'Stuxnet,' which brought the attention of security experts to cyberspace (Farwell & Rohozinski, 2011). The development of Stuxnet elucidates that cyber-attacks go beyond just disrupting critical infrastructure and can have grave consequences for a state's national security. Hence, if the kinetic element becomes part of a cyber-attack, it aligns cyber warfare with the first half of Clausewitz's definition, characterizing it as an *act of force*.

However, let us suppose that cyber-attacks can never cause physical destruction; even then, cyber war fits Clausewitz's idea of an 'act of force.' According to Bassford (2007), Clausewitz's idea of violence is not limited to physical damage and destruction; instead, it shows the presence of 'emotion' (Bassford, 2007). These emotions can also be a part of cyber-attacks and can be the reason for launching cyber operations against an opponent. For instance, many cyber-attacks between India and Pakistan were inspired by changing dynamics between both states. There have been cyber-attacks on Independence Day that sparked nationalist fervor on both sides. Likewise, bilateral tensions also motivate hackers to launch cyber-attacks. Indian hackers reportedly defaced approximately 30 Pakistani websites following Pakistan's announcement of the death sentence for Kulbhushan Jadhav, an Indian spy (Rai, 2017).

As far as 'people' are concerned in Clausewitz's social trinity, it is also noteworthy that in all the cases, people are either direct or indirect victims of cyberattacks or cyber operations. Cyber-attacks have societal implications, including the lack of trust among people in certain companies and authorities to ensure their digital security, the economic losses citizens face, and the hatred spread via hate speech and disinformation on social media (Ashraf & Kayani, 2023). It is also the people who are affected when states carry out propaganda warfare to influence public opinion, as in the case of the 2016 U.S. elections and Russia's cyber warfare against Ukraine since 2022 (Willett, 2023).

War and Combat

Combat is the second most important constituent of war, according to Clausewitz. In the light of the social trinity proposed by Clausewitz, an important part of this element (combat) is the military. In contemporary times, it is evident that the military is playing an important role in cyber warfare. The militarization of cyberspace and Artificial Intelligence (AI) is taking place at an unprecedented pace (Arif, 2021). U.S., China, Russia, and other major powers have integrated cyberspace as a crucial national security component, making it the fifth battlefield. In addition to these states, smaller states are also trying to integrate cyber warfare capabilities and foster their AI militarization to ensure their survival in a rapidly evolving cyber landscape.

The concepts of uncertainty, friction, and the fog of war are closely linked to this aspect of combat and the military domain. Clausewitz emphasized the crucial role of the military in managing the friction inherent in warfare, effectively addressing the associated risks and uncertainties. The notion of uncertainty was later taken up by various scholars of political psychology as well in order to understand the role of perceptions and misperceptions in times of conflict and wars. The prime examples are Lebow and Stein (1995), who studied the Cuban missile crisis from the point of view of provocative deterrence, and Jervis (2017), who emphasized perceptions and misperceptions in international relations. The studies on inadvertent escalation during a crisis were also inspired by Clausewitz's notion of *uncertainty*.

As mentioned earlier, one of the anomalies of cyberspace is that it makes the identification of the attacker difficult, leading to the problem of attribution. This characteristic creates an environment of uncertainty and a fog of war, with the victim unaware of the attacker. Moreover, in cyberspace, it is challenging to maintain deterrence. This is because of the complexities of cyberspace and the identification problem (Geers, 2010). For deterrence to be successful, it is crucial to have significant information about one's capabilities and that of the opponent; however, cyberspace makes it difficult. This argument indicates that uncertainty and the fog of war, which Clausewitz emphasized, are important features of cyberspace, which makes the latter fit into Clausewitz's second element of war, i.e., *combat*.

More importantly, militaries worldwide have been actively conducting cyber operations against the opponents (Lin, 2010). The USA, despite being the champion of free and open internet and cyberspace, has been accused of conducting espionage against its allies and opponents alike, as revealed by Snowden leaks (BBC, 2014). Likewise, China, Russia, Israel, Iran, and other cyber-capable states have also enhanced their offensive cyber capabilities and built their cyber forces/armies to dominate their opponents (Netolicka & Mareš, 2018). However, another school of thought is that because of uncertainty, cyber operations will remain a supportive tool for future wars rather than being a decisive tool. This was evident in the cyber-attacks carried out by Russia during its invasion of Ukraine in 2022 (Mueller et al., 2023).

War as an Instrument of Policy

Propaganda warfare, which uses cyberspace or the Internet, is a clear example of how states use various platforms to advance their national policies, enhance their influence, or shape their opponents' decisions without force. Great powers like the U.S.[5], Russia[6], and China[7] have often used propaganda warfare. Even though propaganda warfare is mainly aimed at influencing the opinion of the masses, not the government, public pressure also has great value for the government. This relates to the use of cyberspace for propaganda warfare which influences the decision-making capability of the opponent.

Cyber-attacks can be used on different levels, from strategic to tactical, and can serve as an important source of political coercion. They can also compel your adversary to do things according to your will (Liff, 2012). Clausewitz's definition mentions that the use of force is primarily to convince your opponent to do your will, making cyber-attacks fit into the latter half of his definition. Abdyraeva (2020) argues

[5] For instance, in 2011, The US military decided to develop software that would let it secretly manipulate social media sites by using fake online personas to influence internet conversations and spread pro-American propaganda.

[6] During the Cold War, the Soviet Union used active measures to influence nations in coercive ways distinct from espionage and counterintelligence. Active measures included disinformation, political influence operations, and controlling media and messaging with the goal of discrediting or influencing the West, which is echoed in Russia's modern-day tactics.

[7] Liu Xiaoming, who recently stepped down as China's ambassador to the United Kingdom, is one of China's most successful foot soldiers on this evolving online battlefield. He joined Twitter in October 2019 and quickly gained popularity on the platform because of his posts and retweets of his posts. Later on, it was found out that the popular support that aimed at influencing public opinion was, in fact, manufactured using fake accounts.

that one of the primary objectives of cyber-attacks is to influence the opponent's will for its national interests using offensive cyber capabilities. More and more states are trying to build strong cyber capabilities because cyberspace enables you to achieve your ambitions without engaging in a military confrontation with other states.

The alleged interference of Russia in the 2016 U.S. national elections to help Trump win the elections is one notable example that signifies how cyberspace can be used to achieve political and national objectives. Russia has long been involved in propaganda warfare and hybrid warfare against the U.S. to contain its spread in the former's surroundings. However, against adversaries grew in Putin's second term—the strategy transitioned from being related to theft to being offensive (Ziegler, 2018). A manifestation of this was the 2016 Russian interference in U.S. national elections.

Notably, cyber warfare does not encompass everyday attacks like cyber espionage and low-scale cyber-attacks but includes cyber-attacks with direct military or political objectives (Liff, 2012). This automatically makes cyber warfare a national security concern. Clausewitz also suggests that *war* is a continuation of politics through other means. The word politics itself needs to be understood more broadly rather than confining it to a narrower concept of politics. Like Clausewitz argues that war is a continuation of politics, it is important to note that politics shape war. As discussed earlier, most cases of Indo-Pak cyber-attacks are caused by bilateral tensions (Green, 2020). The new realm of cyberspace has all the essential components of politics that can be used in a quest for influence and power (Choucri, 2012).

Conclusion

The concept of warfare now incorporates cyber warfare, as does the modern concept of 'security.' Cyberspace has given states a fair chance to stay connected but has also been declared the fifth operational domain for warfare. Certain anomalies like the aspects of anonymity, low cost, non-discrimination in targets, and the involvement of various actors have made cyber security an important constituent of national security. Despite all these factors, some scholars argue that cyber warfare has so far been unable to fulfill the criterion of warfare provided by the traditional realist (Clausewitz). However, an in-depth analysis of Clausewitz's definition and concept of warfare suggests that cyber warfare fits his definition of warfare to a great extent. Thus, cyber security is an issue that needs to be looked upon by the states before their national security is jeopardized.

Conflict of Interest: The author declares no conflict of interest.

Funding: This research received no external funding.

References

Abdyraeva, C. (2020). Cyber Warfare. In *The Use of Cyberspace in the Context of Hybrid Warfare.: Means, Challenges and Trends* (pp. 15-20). OIIP - Austrian Institute for International Affairs. http://www.jstor.org/stable/resrep25102.7

Arif, S. (2021). Militarization of Artificial Intelligence: Progress and Implications. In: Keskin, T., Kiggins, R.D. (eds) *Towards an International Political Economy of Artificial Intelligence.* International Political Economy Series. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-74420-5_10

Ashraf, M. N., & Kayani, S. A. (2023). India's Cyber Warfare Capabilities: Repercussions for Pakistan's National Security. *NDU Journal*, *37*, 34-45. https://ndujournal.ndu.edu.pk/site/article/view/152/114

Bassford, C. (2007). 'The Primacy of Policy and the 'Trinity' in Clausewitz's Mature Thought', in H. Strachan and A. Herberg Rothe (eds*), Clausewitz in the Twenty-First Century* (Oxford, Oxford University Press, 2007).

Bell, C. H. (2018). Cyber Warfare and International Law: The Need for Clarity. *Towson University Journal of International Affairs*, *51*(2). p. 21-43 https://cpb-us-w2.wpmucdn.com/wp.towson.edu/dist/b/55/files/2018/05/SPRING-2018-ISSUE-1zf1eiz.pdf#page=27

Billo, C., & Chang, W. (2004). *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*. Dartmouth University Institute for Security and Technology Studies. http://web.elastic.org/~fche/mirrors/www.cryptome.org/2013/07/cyber-war-racket-0003.pdf

Bussell, J. (2023, October 15). *cyberspace*. Encyclopedia Britannica. https://www.britannica.com/topic/cyberspace

Cavelty, M. D. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics. 20* (3), 701-715. https://doi.org/10.1007/s11948-014-9551-y

Cepik, M., Canabarro, D. R., & Borne, T. (2015). Cyberwar: Clausewitzian Encounters. *Space & Defense-USAF Academy*, *8*(1), 19-33. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144752

Chen, T. M. (2010). Stuxnet, the real start of cyber warfare? [Editor's Note]. *IEEE Network*, *24*(6), 2-3. https://ieeexplore.ieee.org/abstract/document/5634434/

Choucri, N. (2012). *Cyberpolitics in International Relations*. The MIT Press. https://mitpress.mit.edu/9780262517690/cyberpolitics-in-international-relations/

Clarke, R. A., & Knake, R. K. (2010). *The Next Threat to National Security and What to Do About It.* HarperCollins Publishers.

Clausewitz, C. V. (2007). *On War*. Oxford, UK, Oxford University Press.

Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. *India Review*, *19*(4), 376-413. https://doi.org/10.1080/14736489.2020.1797317

Edward Snowden: Leaks that exposed US spy programme. (2014). *BBC News.* https://www.bbc.com/news/world-us-canada-23123964

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on building a community of common future in cyberspace*. Springer. http://file.fouladi.ir/courses/cyber/books/Binxing.pdf

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23-40. https://doi.org/10.1080/00396338.2011.555586

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3), 298-303. https://www.sciencedirect.com/science/article/pii/S0267364910000506

Ghate, S. & Agrawal, P. K. (2017). A literature review on cyber security in the Indian context. *J. Comput. Inf. Technol*, *8*(5), 30-36. https://www.tandfonline.com/doi/full/10.1080/15205436.2017.1382285

Goel, S. (2020). How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. *Connections. 19*(1). 87-95. https://www.jstor.org/stable/26934538

Goldsmith, J. (2010). The New Vulnerability. *The New Republic.* http://www.tnr.com/article/books-and-arts/75262/the-new-vulnerability

Green, K. (2020). Does War Ever Change? A Clausewitzian Critique of Hybrid Warfare. *E-International Relations*. https://www.e-ir.info/2020/09/28/does-war-ever-change-a-clausewitzian-critique-of-hybrid-warfare/

Hadfield, D. (2016). *What Constitutes Cyber War? War and Global Conflict in the Contemporary World.*

Hathaway, M. E. (2008). Cyber Security: An Economic and National Security Crisis. *The Intelligencer: Journal of US Intelligence Studies*, *16*(2), 31-36. https://www.belfercenter.org/publication/cyber-security-economic-and-national-security-crisis

Jervis, R. (2017). *Perception and misperception in international politics: New edition*. Princeton University Press.

Jinghua, L. (2019). What are China's cyber capabilities and intentions? *IPI Global Observatory*. https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Kemp, S. (2020, January 30). Digital 2020: Global Digital Overview. *DATAEPORTAL*. https://datareportal.com/reports/digital-2020-global-digital-overview

Lebow, R. N., & Stein, J. G. (1995). Deterrence and the Cold War. *Political Science Quarterly*, *110*(2), 157-181. https://www.jstor.org/stable/pdf/2152358.pdf

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats* (p. 12). Washington, DC: Center for Strategic & International Studies.

Liff, A. P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, *35*(3), 401-428. https://doi.org/10.1080/01402390.2012.663252

Lin, H. S. (2010). Offensive cyber operations and the use of force. *Journal of National Security Law and Policy*, *4*(63). https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf

Missiroli, A., Stoltenberg, J., & Peach, S. (2020). From hybrid warfare to "cybrid" campaigns: the new normal? In T. Tardy (Ed.), *NATO at 70: No Time to Retire* (pp. 65-72). NATO Defense College. http://www.jstor.org/stable/resrep23663.14

Mueller, G.B. Jensen, B., Valeriano, B., Maness, R.C., and Macias, J.M. (2023). Cyber Operations during the Russo-Ukrainian War: *From Strange Patterns to Alternative Futures*. Center for. *Center for Strategic and International Studies.* https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#h2-russian-cyber-operations

Myers, N. (2020). Cyber Security: Cyber-crimes, attacks, and terrorism. *ODU Model United Nations Society.* https://www.odu.edu/content/dam/odu/offices/mun/docs/1st-cyber-attacks-un-day.pdf

Netolická, V., & Mareš, M. (2018). Arms race "in cyberspace"–A case study of Iran and Israel. *Comparative Strategy*, *37*(5), 414-429. https://doi.org/10.1080/01495933.2018.1526568

Nisar, M. (2018). 5 GW and hybrid warfare its implications and response options. https://bdex.eb.mil.br/jspui/bitstream/123456789/2827/1/MO%200023%20-%20MAAZ.pdf

Otaiku, A. A. (2018). A framework for hybrid warfare: Threats, challenges and solutions. *J Def Manag*, *8*(178), 374-2167. Doi:10.4178/2167-0374.1000178

Paleri, P. (2008). *National Security: Imperatives and Challenges*. Tata McGraw-Hill.

Panwar, R. S. (2017). The Changing Nature of Warfare - Part II. *Future Wars.* http://futurewars.rspanwar.net/the-changing-nature-of-warfare-part-ii/

Poindexter, D. F. (2015). *The new cyberwar: Technology and the redefinition of warfare*. McFarland.

Rai, A. (2017). Tit for tat hack attack! Pakistan black hats hit back after Indian cyber strike to avenge naval officer's death penalty. *Mail Online India*. Retrieved from http://www.dailymail.co.uk/indiahome/indianews/article-4445606/Pakistan-black-hats-hit-Indian-cyber-strike.html

Renz, B. (2014). Russian Military Capabilities after 20 Years of Reform. *Survival*, *56*(3), 61-84. https://doi.org/10.1080/00396338.2014.920145

Renz, B. (2016). Russia and 'hybrid warfare.' *Contemporary Politics*, *22*(3), 283-300. https://doi.org/10.1080/13569775.2016.1201316

Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5-32. https://doi.org/10.1080/01402390.2011.608939 .

Sharma, D. (2011). China's Cyber Warfare Capability and India's Concerns. *Journal of Defence Studies. 5*(2), 62-76. http://www.idsa.in/system/files/jds_5_2_dsharma.pdf

Subramanian, R. (2020). Historical Consciousness of Cyber Security in India. *IEEE Annals of the History of Computing*, *42*(4), 71-93. https://ieeexplore.ieee.org/

Syed, F. Z., & Javed, S. (2017). Deterrence: A Security Strategy against Non-Traditional Security Threats to Pakistan. *International Journal of Social Sciences and Management*, *4*(4), 267-274. https://doi.org/10.3126/ijssm.v4i4.18503

Tiirmaa-Klaar, H. (2011). Cyber security threats and responses at global, nation-state, industry and individual levels. *Ceri SciencesPo*, 1-10. https://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/art_htk.pdf

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA.

Willett, M. (2024). The cyber dimension of the Russia–Ukraine war. *Adelphi Series*, *64*(511–513), 105–124. https://doi.org/10.1080/19445571.2024.2417541

Wilson, C. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress*. Library of Congress Washington DC Congressional Research Service. https://corpora.tika.apache.org/base/docs/govdocs1/080/080803.pdf

Wu, Y., & Huang, Y. (2020, August). Will Cyber Warfare Become a Threat to Contemporary International Security? In *2020 4th International Seminar on Education, Management and Social Sciences (ISEMSS 2020)* (pp. 31-34). Atlantis Press. 10.2991/assehr.k.200826.007

Ziegler, C. E. (2018). International dimensions of electoral processes: Russia, the USA, and the 2016 elections. *International Politics*, *55*(5), 557-574. https://doi.org/10.1057/s41311-017-0113-1