International Research Journal of Social Sciences and Humanities, Vol.:03, Issue: 02,July-Sep,2024
PP:345-357

OPEN ACCESS
IRJSSH
ISSN (Online): 2959-1392
ISSN (Print): 2959-2887
www. irjssh.com

CYBERSECURITY AS A GEOPOLITICAL TOOL: THE GROWING INFLUENCE OF DIGITAL WARFARE IN STATECRAFT

Aneel Waqas Khan
Visiting Lecturer, Government College University, Lahore.
Email: *aneelwaqas@yahoo.com*

Dr. Sarah Saeed
Lecturer, Humanities Department, COMSATS University Islamabad.
Email: *sarah.saeed@comsats.edu.pk*

M. Saleem Kakar
(Corresponding Author)
Lecturer, Humanities Department, COMSATS University Islamabad.
Email: *Saleem.kakar@comsats.edu.pk*

Abstract

Cybersecurity is now an integral part of geopolitical strategy, and digital warfare has emerged as a weapon both of power projection and of national defense in the digital age. This article examines how cyber capabilities in the form of espionage, infrastructure sabotage, and information manipulation, have exerted new forms of influence and disrupted traditional power dynamics and have changed statecraft in and of themselves. The article takes as its point of departure prominent cyber incidents, including Russia's reported interference in Western elections and cyber-attacks on critical infrastructure in Asia and the Middle East, to examine how states utilize cyber tools to pursue strategic objectives while precluding military conflict. The piece also goes on to assess the implications of cyber warfare on international relations, and how states are responding to these threats with alliances, international regulations, and defensive capabilities. This article ends by presenting the different facets of the dual role of cybersecurity both as a defensive shield and as an offensive tool, asking questions about the future dynamics of global stability and digital geopolitics in the making.

Keywords: *Cybersecurity, Geopolitical, Digital warfare, Western elections, Statecraft.*

CYBERSECURITY AS A GEOPOLITICAL TOOL: THE GROWING INFLUENCE OF DIGITAL WARFARE IN STATECRAFT

INTRODUCTION

In contemporary cyber age cybersecurity has come up as a major factor in deciding how states communicate, wage and undertake war, as well as protect their interests. Modern financial systems, communication networks and national infrastructures, which are increasingly being digitized, are becoming increasingly exposed to cyber threats. However, cyber capabilities are now essential parts of national security strategies, while digital warfare is increasingly being considered an essential instrument of statecraft. The reasons for this shift have been, simply, that cyber-attacks are extremely low cost, extremely high impact and extremely deniable, making them an ideal tool for states looking to secure strategic goals in ways other than through the risks of conventional conflict.

The defining aspect of cyber warfare is its capacity to breach established defense systems and immediately go after a state's political, economic and social structures. The United States and Israel were supposedly behind the Stuxnet virus, which was allegedly designed to disrupt Iran's nuclear program with incredible precision, and was used as the model for how cyber tools could be used for selectively sabotaged industrial infrastructure. Just as an example, cyber interference in elections, and in particular Russia's alleged influence on the 2016 U.S. presidential election, shows how cyber capabilities can affect political process and public states of mind without direct invasion. These incidents highlight the unique power of cyber tactics: however, as attribution can be difficult and the impact on the core functions of a nation can be significant, while granting plausible deniability to the attackers, attribution is often complex and with minimal repercussions for the attackers.

The lack of international regulation in the field of cyber warfare makes the complexity of managing cyber warfare even greater. Unlike conventional warfare, where there are rules of engagement, such as in the form of treaties, written as the Geneva Conventions, that govern cyber warfare. In the gray zone of the laws of cyber capabilities, states game their ability to exploit the very technology that facilitates cyber aggression without accountability. Trying to deal with these kinds of challenges, some states have started calling for cyber norms, but major progress is lacking. For example, the United Nations Group of Governmental Experts has undertaken to create such norms concerning responsible state behavior in cyberspace, but finding consensus has been difficult due to competing national interests and the dark secret of cyber capabilities.

As countries are responding to growing cyber threats, more and more are striving to enhance their cyber defense and offense. The buildup of dedicated cyber forces in military and intelligence services around the world, like the United States, China and Russia have turned into digital arms races. In addition, cyberspace is deemed as an operational domain by alliances like NATO and member states of NATO can respond collectively on the cyber threats. The militarization of cyberspace as a response for future conflicts acknowledges that cyber warfare is an ongoing part of future conflict and needs technical infrastructure as well as strategic alliances to deter future adversaries.

Regarding the increase of cybersecurity as a geopolitical strategy tool this article analyzes how cyber warfare plays a role in global security and state relations. It lays out the effect of cyber capabilities on modern statecraft by exploring key incidents, policy responses, and shifts in the character of cyber threats. By doing so it considers some of the most urgent questions about how war and peace unfold in the era in which lines continue to blur between espionage, technology creates new forms of war, and cyber warfare continues to exert a pervasive, covert and ultimately destabilizing influence. To comprehend the intricacies of the evolving digital geo-political landscape and the far wider implications of cybersecurity in global politics we must grasp these dynamics.

REVIEW OF THE LITERATURE:

A literature review on the role of cybersecurity as a tool of geopolitics illustrates the rising importance of digital war in the practice of modern international relations, among other facets of national security and complexities for the regulation of cyber activities of the states.

States have been using cyber capabilities to realize a variety of strategic goals, and in a way that does not require traditional military engagement. Scholars like Nye (2011) motivate the use of cyberspace to obtain objectives by changing or influencing other actors' behaviors is a crucial part of power for states. Whereas conventional power dynamics are constructed in an arena where attribution can be challenging along with ambiguous consequences, cyber power facilitates states' subtle, strategic use of influence (Nye, 2011). As a result, cyber tools have been used for, ranging from espionage to influence operations, thus raising cybersecurity as a major geopolitical concern (Libicki, 2009).

This research touches on how cyber warfare has such an influential role in national security. As landmarked in the use of cyberspace weapon for strategic benefit, Clarke and Knake (2010) elaborate the vulnerability of national infrastructure to cyberspace attacks including the case of the Stuxnet

virus aimed against Iran's nuclear program. These kinds of instances are a demonstration of how digital warfare can get around traditional defenses and instantly damage the critical infrastructure. Changing nature of cyber threats realized also often includes actors state and nonstate, underscore the priority of the development of integrated cybersecurity policies (Clarke & Knake, 2010; Lindsay, 2013).

Attribution is a huge problem because it is so difficult, and there is no clear legal framework that exists around cyber things. As Rid and Buchanan (2015) put it, cyber-attacks are difficult to trace and lack sufficient evidence to allow for accountability and to inhibit diplomatic responses. This lack of accountability encourages states to use Lasers. Lack of accountability encourages states to use the lasers without having to worry about repercussions. Secondly, the lack of universally accepted legal standards for cyber warfare compounds these challenges by providing regulatory vacuum. International efforts, typical in the Tallinn Manual, try to export the use of international law into cyberspace, while states are not and never were able to reach consensus on this matter, since cyber warfare is a matter of complex and ever evolving nature (Schmitt, 2013).

In today's context of a "cyber arms race" among major powers, several scholars define it as both a defensive and an offensive cyber power (Healey, 2013). For example, the United States and China have rushed to build big cyber warfare units, and NATO has acknowledged cyberspace an operational space for collective defense. The implications for international stability are that states might resort to a preemptive cyber strategy considering a fear of attack (Libicki, 2009). According to some studies, international cooperation in cybersecurity is technically feasible and necessary, while at the same time largely difficult to execute, and multilateral efforts could mitigate the risk of escalation with cyber conflict (Maurer, 2018).

Cybersecurity holds geopolitical implications: alliances are shaped, national securities policies are drawn up, so is the definition of sovereignty in the cyber world (Nye, 2011). As cyber capabilities increase, the potential for cyber conflicts to extend into physical confrontations increases too, some say, and that is why there's a need for robust international agreements. Reducing the risk of escalation through the development of norms of responsible behavior in cyberspace is seen as important to long term global stability (Lindsay, 2013).

METHODOLOGY:

For the purposes of this research, a qualitative methodology is used to explore the function of cybersecurity as a geopolitical tool, using digital warfare as a strategic tool in international relations. For this study a case study approach will be adopted selecting key instances of cyber incidents attributed to state actors. The research explores the outcome of cyber cases with motivation for motivation, a strategy for strategy, and an implication of implication to state craft.

The first aspect of the research will be to study several important cyber incidents which demonstrate the use of cyber capabilities for geopolitical purposes. Examples of such development include Iranian nuclear facilities targeted by Stuxnet attack, which is an example of how states can use cyber tools to damage critical infrastructure (Clarke & Knake, 2010). Furthermore, the use by Russia of cyber capabilities during its interference into the 2016 U.S. presidential election is another significant case of using cyber capabilities to affect political processes and influence public opinion (Lindsay, 2013). Finally, the economic motivations, namely, cyber activities by state, for North Korean cyber-attacks on financial institutions will be illustrated (Healey, 2013). They are cases that matter, complex, speaking to the intersections of cybersecurity and geopolitics.

Gathering the main data for this qualitative analysis will be from a variety of sources. Included are government reports, policy documents and legislative hearings which will provide information about the government army facing cyber threats. Furthermore, academic journal articles, books and credible news outlets will also be reviewed to provide a wider understanding of the implications of these cyber-attacks. This permits the integration of expert analysis and data to build up a comprehensive perspective on the strategic way cybersecurity is used in statecraft (Nye, 2011).

Qualitative content analysis will be used for the research, which will examine the selected case studies. Simply to code and categorize these incidents on several dimensions such as the type of cyberattack involved (espionage, sabotage), the strategic objectives pursued and responses from the targeted states and the international community. The analysis will identify how states use cyber capabilities to realize a particular set of goals, for example, political influence, economic advantage or technological superiority (Rid & Buchanan, 2015). The takeaway of this method will be that research is able to make grounded conclusions regarding the nature and consequences of digital warfare in global geopolitics.

Besides individual case studies, a comparison analysis would be carried out to identify the similarities and the dissimilarities in the selected incidents. How the geopolitical context, who the actors are, and what the targets are is, will play a role in the use of the subtle force of cyber capabilities will be explored in this analysis. The research contrasts these cases to reveal broader trends in cyber warfare and how states make strategic calculations concerning their electronic actions (Schmitt, 2013). This thesis will shed light on the changing landscape of international relations and the security implications for national security that results from such cybersecurity.

The qualitative approach is also concerned with validity and the ethical considerations in interpretation of data. The research will take place with documented cases and credible sources to obtain reliability. The ethical considerations involve being accurate and fair to the representation of sensitive geopolitical data when addressing whether certain cyber activities are contentedly attributed. The research will subject cyber warfare to a critical evaluation, considering all the complexity and uncertainty associated with cyberspace (Clarke & Knake, 2010; Nye, 2011).

This research employs a qualitative methodology based on case studies to look into how cybersecurity is used as a tool of statecraft in the modern geopolitical context and offers insights of this kind through case studies. The findings will help better understand the strategic role of cyber capabilities in international relations, and the implications for global security more broadly.

ANALYSIS:

The realm of cybersecurity has emerged as a critical aspect of contemporary geopolitics, fundamentally altering the dynamics of statecraft. With the proliferation of digital technologies, nations are increasingly engaging in cyber operations to advance their strategic interests, shaping the landscape of international relations and security.

CYBER OPERATIONS AND STATECRAFT:

Also, the security of our nation's information networks now matters as much as the air we breathe or water we drink. Viewed primarily as defensive measures, Cyber has recently been used offensively through Statecraft to conduct espionage, disrupt adversaries, and to influence foreign and domestic narratives. It shows the way in which cyber power has come to play a role in achieving strategic objectives without conventional military conflict (Nye, 2017; Sullivan, 2022). For example, espionage and data theft enable states not only to

learn critical things regarding adversaries but to obtain strategic advantage in the economic and political domains. This tactic is particularly applicable to Chinese cyber espionage efforts to get technology from Western firms to give themselves an advantage in their competitive playing field on the world stage (Segal, 2018; Libicki, 2020).

New avenues for coercion and deterrence have been added by cyber capabilities. Digital warfare is here, and states are using it to insert messages into the digital landscape, and send out targeted signals at adversaries to project dominance in the digital realm, which many say is one of the most meaningful there are. Cyber operations are often covert, less costly to conduct than traditional military operations, and even afford plausible deniability complicates fiduciary frameworks of accountability and response in international relations (Buchanan, 2020). Cyber incursions into Ukraine's power grid, for example, as with cyberattacks on critical infrastructure in general, represent ways in which cyber tools can alter conflict outcomes without the deployment of conventional military forces (Rid, 2012). These efforts, known as "gray zone," activities, make use of the grey area between peace and conflict to work at projecting state power and preventing adversaries from escalating into open warfare (Eriksson & Giacomello, 2021).

Cyber tactics, in turn, are generating new demands on traditional notions of sovereignty and state borders. Unlike conventional warfare, cyberattacks are not tied to geography so states could strike from afar without crossing geographical borders. That has prompted discussions on what counts as an act of war in the digital era. For example, NATO acknowledges that Article 5 may apply in response to major cyberattacks, in which regard it counts cyber incursions as acts of armed attack under certain circumstances (Schmitt, 2017). The redefinition is a telltale indication of how cyber warfare has revolutionized international security protocols and responses (Sulmeyer, 2018).

Furthermore, cyber tools in statecraft have affected a rethinking of global and defense strategies. Because cyber capabilities appear to increasingly be considered the heart of national power, NATO and other national alliances and partnerships are changing to incorporate cyber defense as an area of vital cooperation. In response, countries are forging coalitions to set norms and framework for cyber engagement with the hope of reducing the risks of unregulated cyber (Buchanan, 2020; Nye, 2017). Yet international norms on cyber conduct remain underdeveloped, leaving states free to unilaterally and without transparency engage in cyber activities, without accountability.

Cascading with it are cybersecurity and its impact on international diplomacy. Cyber has blurred lines between states' peacetime activities and the act of war, making it difficult (and perhaps undesirable) for states to draw clear rules and responses. The emergence of cyber capabilities as instruments for pressures place a premium on establishing universal consensus on acceptable cyber conduct and the tools for responsibility (Eriksson and Giacomello, 2021). Today, the international community must deal with the ethics, law, as well as strategic ramifications of cyber operations, and try to avoid an unregulated cyber arms race (Rid, 2012; Zetter, 2014).

THE RISE OF DIGITAL WARFARE:

States are increasingly using hacking, cyber espionage and disinformation campaigns as part of their digital warfare repertoire to affect global affairs and further their agendas. State sponsored cyber operations are capable of subverting democratic processes – manipulating the perception of the public in pursuit of strategic wins (Sullivan, 2022). By employing a mix of disinformation campaigns and hacking, Russian operatives were able to sow discord amongst the American electorate, damaging faith in democratic institutions and acting on public opinion—an act which has been widely criticized for its perceived damage to electoral integrity (Rid, 2019; Greenberg, 2019). This is an effective strategy of digital tools, which shows what can never be with traditional, reshaping public sentiment all over the world and being a powerful signal of modern warfare tactics.

Like digital warfare, China is also all of arms, its cyber activities to U.S. corporate and government networks aiming for both economic and strategic advantage. Major hacks such as those against the Office of Personnel Management (OPM) and Equifax have exposed Chinese cyber espionage campaigns aimed at stealing the Secret, the Top Secret, and Special Access Program (SAP) data of foreign nationals to feed it to foreign espionage and blackmail (Kello, 2017). These activities illuminate the strategic importance of cyber capabilities, which differ from weapons of war in that the very information being captured is intellectual property (Singer & Friedman, 2014). Since in digital warfare, information and economic dominance can be pursued while bypassing physical warfare, such data theft endorses an economic edge (Segal, 2018).

But disinformation as a tool of digital warfare has proved effective not just against election interference, as Russia has weaponized it to mangle NATO alliances and enforce public opinion in Eastern Europe. Russia aims to create

rifts between the countries of NATO, in order to divide and weaken the alliance from within through coordinated disinformation campaigns (Chivvis, 2017). Digital warfare, it finds, knows no borders and it plays on a country's political stability and alliances by wrecking public confidence among allies and destabilizing their political discourse. Given the low cost and high impact of such tactics, states have been particularly attracted to these kinds of disruptive actions, which can be taken without triggering traditional military response (Buchanan, 2020).

Digital warfare is increasingly used as a determent tool beyond political influence. To date a subcategory of this traditional strategy towards military organization has gained momentum and manifested in a term known as 'hybrid warfare' where states use a combination of cyber, military and digital tools to exert influence without direct brinkmanship (Eriksson & Giacomello, 2021). One example of such a state use of cyber tools was the cyberattack (putatively conducted by Russian actors) that disrupted Ukrainian critical infrastructure on a massive scale and damaged their economy and infrastructure with little risk of crossing the war threshold (Greenberg, 2019). This cyber approach is a new dimension to military strategy that shows how digital warfare can cripple an opponent by attacking its most important networks and critical infrastructure.

Such growing influence of Digital Warfare is not just bringing a new face of international conflict but is creating a vacuum of the need for regulatory measures as well as international norms. While cyber tools reshape the trends of modern geopolitics, states and international organizations are being forced to develop frameworks of cyber conduct and accountability for cyber aggression (Sulmeyer, 2018). The escalation of cyber conflicts remains particularly salient because, without comprehensive agreements and cooperative defenses, technological innovation and geopolitical stability play a far more intricate interplay (Nye, 2017).

THE IMPACT ON INTERNATIONAL RELATIONS:

By integrating cyber capabilities into the realm of statecraft, new aspects of conflict and diplomacy are brought into the picture, and fundamentally reshape the landscape of international relations. However, unlike traditional warfare, physical boundaries demarcate national security across states, but cyber operations do not, instead they permit states to influence, disrupt or manipulate another state's systems from afar rendering the line between operations that are peacetime and acts of war (Nye, 2017). Yet this ambiguity presents a challenge for international law and conflict resolution, particularly because ascertaining the identity of the principal actors in cyber incidents is by

no means a simple undertaking, and cyberattacks are not well regulated, whereas norms of traditional military aggression are (Libicki, 2009). The resulting 'gray area' of cyber operations necessitates new frameworks for identifying and responding to cyber threats while keeping the global balance (Clarke & Knake, 2019).

This ties into the fact that as digital tools mature, they provide states with covert mechanisms for effecting influence that generate less visible costs and negative consequences than conventional force would, making diplomatic forward deployment all the harder. As countries utilize these cyber tools to show political stance, to apply economic pressure or disrupt foreign infrastructure they can do so without declaring war, increasing the likelihood of misunderstandings and escalations in international conflicts (Kello, 2017). Increased deployment of advanced malware in global critical infrastructure makes this risk particularly apparent as there is a potential for misinterpretation of who is behind any given attack, thereby triggering the inadvertent retaliation which can only escalate further a highly unstable diplomatic situation (Buchanan, 2020).

Also, as non-state actors including hacker groups and terrorist organizations are emerging, the cyber landscape is becoming complex. Unlike state actors, one of these groups' goals may be ideological or financial; it can also lack national interest, making its actions unpredictable and potentially destabilizing (Arquilla & Ronfeldt, p. 2001). Cyber security vulnerabilities are exploited by non-state actors across borders to push their agendas, whether some of them are unwittingly implicating states and making international relations more difficult to sort through. Groups like Anonymous or terrorist organizations have used the cyber means to attack the financial systems, government websites, critical infrastructure, crossing the boundary between accountability, and pushing traditional state-centric defense frameworks (Rid, 2019).

Because no single state can fight cyber threats alone, these actors require more enhanced international collaboration. With cyber threats crossing national borders, it has become recognized by both countries where cooperative defense strategies, common intelligence and unified cyber norms must go. The United Nations and other international bodies also advocate for cybersecurity norms which would lessen the risk of miscalculation and further an understanding of what roles states and non-state actors play in cyber warfare

(UN General Assembly, 2015). But states tend to vary in their cyber policies as well as levels of transparency, so it's challenging to create universally binding regulations (Singer & Friedman, 2014).

Finally, the development of cyber capabilities in statecraft demonstrates in the end the requirement to alter diplomatic and legal approaches of warfare to frame and govern this new domain of struggle. The solution path for nations involved in cyber operations includes both the issues of sovereignty and the international law behind it while the international community is challenged with striking this balance of the technological advancements and requirements for stability, security, and accountability within the space of cyberspace. This high potential for conflicts to spill over into the digital realm, with lasting consequences for global peace and security, remains without clear policies and agreements (Libicki 2009, Sulmeyer 2018).

CONCLUSION:

In conclusion, cybersecurity has emerged as an indispensable tool of modern statecraft, significantly impacting the geopolitical landscape by transforming traditional power dynamics and introducing new challenges to international stability. The expansion of digital warfare capabilities, such as cyber espionage and disinformation campaigns, has provided states with a means of influencing, deterring, and even destabilizing adversaries without direct military engagement (Buchanan, 2020). Cyber operations offer a strategic advantage through anonymity and deniability, complicating attribution and blurring the line between wartime and peacetime actions. As incidents of cyber operations grow, they emphasize the need to address cybersecurity as a central facet of national defense and international relations (Nye, 2017; Clarke & Knake, 2019).

The rise of non-state actors in the cyber domain has further exacerbated the complexity of the cybersecurity landscape. Unlike state-sponsored operations, the motivations of these groups are often unpredictable, including financial gain, ideological causes, and even anarchistic disruption. These actors' activities can challenge state authority and create unintended conflicts between states, thereby underscoring the limitations of conventional security frameworks in addressing cyber threats (Arquilla & Ronfeldt, 2001; Rid, 2019). Additionally, the fluidity of cyber operations enables these actors to transcend national borders, making cyber threats a truly global issue that requires coordinated responses across states and international institutions (UN General Assembly, 2015).

Addressing the challenges posed by digital warfare and cyber threats demands a comprehensive rethinking of traditional approaches to diplomacy, deterrence, and defense. A unified international framework for cyber operations is critical to maintaining stability in the digital sphere. However, the divergent policies and security priorities of states create obstacles to establishing such agreements. For example, while some countries advocate for a rules-based order in cyberspace, others prioritize sovereignty over transparency, complicating consensus-building on universal norms (Singer & Friedman, 2014; Nye, 2017). The ongoing attempts by organizations like the United Nations to create cybersecurity norms reflect the urgency and difficulty of balancing national interests with global security (Sulmeyer, 2018).

Ultimately, as cybersecurity becomes more integral to national security, states must consider how to balance offensive and defensive capabilities. While defensive measures are essential to protect state infrastructure and prevent cyber incidents, the pursuit of offensive capabilities can escalate tensions, leading to a potential arms race in cyberspace. The dynamics of cyber power and deterrence in this context are complex, as retaliation and escalation are often ambiguous in the cyber realm, making the rules of engagement unclear (Libicki, 2009; Buchanan, 2020). Thus, states face the challenge of developing a stable and enforceable cyber strategy that minimizes conflict and fosters resilience against cyber threats.

In summary, cybersecurity's role in statecraft is transformative yet fraught with complexities. The integration of cyber capabilities into geopolitical strategy redefines notions of conflict, sovereignty, and international law, urging the global community to devise mechanisms for cooperation and regulation. As technology advances, so too will the sophistication of cyber threats, necessitating adaptive, collaborative, and forward-looking solutions to maintain international peace and security in an increasingly digital world (Clarke & Knake, 2019; Kello, 2017). The future of cybersecurity as a tool of statecraft will depend on states' ability to foster an international consensus that addresses the realities of digital warfare, balancing national interests with the collective need for security and stability.

References

1- *Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror,*

Crime, and Militancy. RAND Corporation.
2- *Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press.*
3- *Chivvis, C. S. (2017). Understanding Russian "Hybrid Warfare" And What Can Be Done About It. RAND Corporation.*
4- *Clarke, R. A., & Knake, R. K. (2019). Cyber War: The Next Threat to National Security and What to Do About It. Ecco.*
5- *Eriksson, J., & Giacomello, G. (2021). International Relations and Cyber Security. Routledge.*
6- *Greenberg, A. (2019). Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Doubleday.*
7- *Kello, L. (2017). The Virtual Weapon and International Order. Yale University Press.*
8- *Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.*
9- *Libicki, M. C. (2020). Cyber Deterrence and Cyber War. RAND Corporation.*
10- *Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. International Security, 41(3), 44-71.*
11- *Nye, J. S. (2017). The Cyber Revolution and International Relations. The Washington Quarterly, 40(4), 7-20. https://doi.org/10.1080/0163660X.2017.1392064*
12- *Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32.*
13- *Khan, M. B., Saad Jaffar, D. I. N., Mukhtar, M. W., & Ahmed, W. (2023). Nature Of 21st Century's Global Conflicts Under The Global Powers' Geoeconomic Strategies And Islamic Ideology For Peace. Journal of Positive School Psychology, 1291-1298.*
14- *Rid, T. (2019). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.*
15- *Schmitt, M. N. (2017). NATO's Cyber Defense. International Law Studies, 93, 437.*
16- *Segal, A. (2018). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. PublicAffairs.*
17- *Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.*
18- *Sulmeyer, M. (2018). Defending Forward: The 2018 Cyber Strategy is Here. Lawfare.*
19- *Sullivan, D. (2022). Cybersecurity as a Geopolitical Tool. Foreign Affairs.*
20- *Khan, M. B., Jaffar, S., Sajid, S., Amaria Atta, W. A., & Mukhtar, M. W. (2024). Alone Atomic Islamic State Pakistan's Significant Geo-Political Location For Super Powers Monopole Strategies Cultivation. Kurdish Studies, 12(4), 1537-41.*
21- *Sullivan, G. (2022). Cybersecurity and Geopolitics. Cyber Defense Journal.*
22- *UN General Assembly. (2015). Developments in the Field of Information and Telecommunications in the Context of International Security.*
23- *Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown.*

.