SECURITY IN THE FIFTH DOMAIN: REALISM IN CYBERSPACE

Hussain Muhammad
PhD Scholar
Department of Politics and International Relations
International Islamic University
Islamabad-Pakistan
hussain.phdir53@iiu.edu.pk

Prof. Dr. Muhammad Khan
Professor
Department of Politics and International Relations
International Islamic University
Islamabad-Pakistan
drmkndu1964@gmail.com

Abstract

The rapid evolution of cyberspace has drastically transformed the landscape of international relations by its unconventional SWOT matrix and a highly fluid operational environment, which left traditional theories whose assumptions are rooted in the physical domain struggling to catch up and account for the rapid pace of change. As a nonphysical domain, it overcomes the stopping power of geography by transcending borders and temporal constraints by ensuring an instantaneous and real-time flow of information. Additionally, it has created new conflicts that have fundamentally disrupted the conventional notions of power, security, and sovereignty. These changes along the spatial and temporal lines, and the uniquity of this fifth domain raises new questions about the state centrism, territorial sovereignty, and military power in an anarchic system. This article explores how the emergence of this fifth domain has challenged the key assumptions of realism and how realist scholars have tried to catch up with the pace of developments in this inherently disruptive domain.

Keywords: Cyberspace, Fifth Domain, Cybersecurity, APT, DDoS

Introduction

The idea that advances in information and communications technologies had serious implications for national security first came into consideration before the spread of the Internet in its current form and the U.S. Department of Defense (DoD) ARPANET was only 15 years old at

the time. Ronald Reagan was the first American president to sense the drastic impact of computer systems on national security. Interestingly, this realization came after watching a movie in June, 1983. In this movie (WarGames) a young hacker breaches into the nuclear response system of the NORAD (North American Aerospace Defense Command) and this intrusion pushes United States and Soviet Union to the brink of a nuclear war. (Kapell & Elliott, 2013, p. 284) The scenario in the movie was discussed with the national security staff, and the question at hand was about the possibility of such breaches. Most of the national security officials were skeptical because a few months ago, the president had asked scientists to materialize his Star Wars vision by making laser weapons that could shoot incoming Soviet nuclear ballistic missiles. However, despite the prevailing skepticism, the Chairman of the Joint Chiefs, General John Vessey, assured to investigate it.

After investigating Gen. Vessey reached a starkly different conclusion. The likelihood and potential impact of such breaches were far greater than initially expected. This led the entire national security apparatus in a new direction and consequently the National Security Division Directive (NSDD-145) was signed in September 1984 as the 'National Policy on Telecommunications and Automated Information Systems Security.(Kaplan, 2016, p. 2) Reagan's question, in essence, was what later developed into a specialized field of cybersecurity.

Security in the Digital Realm

The problem of security is rooted in the pathology of cyberspace because network information systems were not envisaged and designed with the intention of being secure but efficient, and there is always a tradeoff between usability and security. A completely secure system is dysfunctional, and every usable and functional system has its own shortcomings in terms of security.(Cranor & Garfinkel, 2005, p. 18) The first effort to grasp the new reality was by Arquilla and Ronfeldt when they developed the ideas of netwar and cyberwar and signaled a new kind of contest in a domain that was inherently different from other domains which gradually evolved into a subdiscipline of cyber international relations.(Arquilla et al., 1997) The rise of cyberspace as a crucial arena for state engagement introduces novel complexities and prospects for realist interpretation. The advent of cyberspace as the fifth domain of warfare has posed significant challenges to the realist theory which traditionally emphasizes state sovereignty, military power, and the anarchic nature of the international system. Realism, with its focus on state-centric power dynamics and the pursuit of national interests, struggles to adequately account for the complexities introduced by cyberspace, where non-state actors, transnational networks, and information fluidity play pivotal roles. One of the primary challenges of realism is the diminished relevance of territoriality in cyberspace.

Choucri contends that the fluidity and anonymity inherent in cyberspace undermine the traditional notions of borders and boundaries, which are central to realist thought(Choucri, 2012). In this digital realm, state actors often find their sovereignty challenged by non-state entities, such as hackers and cybercriminal organizations, which can operate across borders with relative impunity. It complicates the realist perspective, which relies on the assumption that states are the primary actors in international relations, and that their interactions are governed by power politics.

Moreover, the nature of conflict in cyberspace differs markedly from that of conventional warfare, which is a core concern in realism. Cyberattacks can be executed with minimal resources and can target critical infrastructure without the need for large military forces. This shift is highlighted by Levy and Gafni, who discuss the challenges of assessing the impacts of cyberattacks, arguing that the traditional metrics of military power do not apply in the same way in cyberspace.(Levy & Gafni, 2021)

Receding State-centrism?

The ability of smaller, less powerful actors to inflict significant damage through cyber means challenges the realist assumption that military capability is the primary determinant of state power. The threshold between an information security incident and international security is elusive but if the strategic gain/loss is significant for actors, it can lead to the actual use of military force. The anomaly of asymmetric gain and loss is at the center of cyberspace. As an inherently different domain it introduces a normal curve for actors of starkly different capabilities. By doing this, cyberspace creates a paradoxical scenario by amplifying both the severity and spread of threats to nations with higher automation and any adversary can launch crippling attacks on their critical infrastructure while states with lower levels of automation that rely mostly on legacy technologies are relatively immune to complex cyberattacks.

In addition, the role of international cooperation in addressing cybersecurity issues further complicates the realist framework. Realism posits that states primarily act in their self-interest, often leading to competition and conflict but the transnational nature of cyber threats necessitates collaboration between states and non-state actors to develop effective responses. Deibert and Rohozinski noted that while states may cooperate in certain cybersecurity policies, divergent national interests can lead to conflicting approaches, highlighting the limitations of a purely realist perspective(Deibert & Rohozinski, 2010). This need for cooperation suggests a more complex interplay of interests, which realism does not fully capture. Similarly, the emergence of public-private partnerships (PPPs) in cybersecurity illustrates a shift in the locus of authority and responsibility away from the state. As organizations increasingly rely on private sector expertise to manage cyber threats, the traditional realist view of state sovereignty and control is challenged. It is important to involve multiple stakeholders in cybersecurity efforts because effective governance in this domain requires a collaborative approach that transcends state-centric models(Kour et al., 2019). This trend reflects a broader shift towards recognizing the role of non-state actors in global governance, which realism tends to overlook. As the international landscape continues to evolve in response to cyber threats, a re-evaluation of existing theoretical frameworks may be necessary to better understand the complexities of contemporary global security.

Realist perspectives on cyberspace emphasize the continuity of power politics, importance of state sovereignty, and strategic significance of cyber capabilities. They view cyberspace as a new domain of competition and conflict, necessitating robust cyber defense and strategic deterrence to protect national interests. Cyberspace, as the fifth domain, has significantly challenged several key assumptions of realist theory in international relations and its emergence has disrupted traditional notions of state sovereignty and territorial integrity, which are

fundamental to realist theory. In cyberspace, national borders become less relevant, and states' ability to control their territory is diminished.(Choucri & Goldsmith, 2012)

Sovereignty in the Digital Realm

This erosion of sovereignty is particularly relevant in the context of international cyber norms and governance, in which states navigate a complex landscape of competing interests and values. Choucri's exploration of the intersection between cyberspace and international law reveals how traditional legal frameworks struggle to adapt to the reality of the digital age. The ambiguity surrounding accountability and attribution in cyberspace further complicates the realist focus on deterrence and retaliation, as states may find it challenging to respond effectively to cyber threats when the aggressor's identity is obscured.(Choucri & Clark, 2019) This uncertainty can lead to miscalculations and escalation, which are critical concerns for realists who prioritize stability and predictability in international relations. Her analysis illustrates that cyberspace significantly influences realist theory by reshaping power dynamics, complicating security concepts, challenging state sovereignty, and highlighting the limitations of traditional legal frameworks. As the digital landscape continues to evolve, the implications for realist thought will likely deepen, necessitating a re-evaluation of established theories to account for the complexities introduced by cyberspace.

Lucas Kello argues for treating cyberspace as a structural modifier in international relations, which has implications for realist theory. This approach suggests that cyberspace influences state behavior within the existing international structure rather than completely revolutionizing it. For realist theory, which emphasizes the importance of state power and security in an anarchic international system, cyberspace alters the nature and number of interactions between states but does not fundamentally change the core principles of realism. Kello's view contrasts with some other perspectives that see cyberspace as a revolutionary force in international relations. By treating it as a structural modifier, he maintained that cyberspace operates within the confines and constraints of the existing structure, which aligns more closely with realistic assumptions about the persistence of anarchy and state-centric power dynamics.(Foulon & Meibauer, 2024) Kello's approach suggests that while cyberspace impacts areas such as deterrence, foreign policy tool choice, and uncertainty it does not fundamentally overturn realist principles. Instead, it modifies how these principles operate within the existing international structure, requiring policymakers to consider cyberspace alongside other domains of statecraft rather than in isolation(Foulon & Meibauer, 2024). However, he contends that the Clausewitzian framework is inadequate for understanding cyber threats, as it fails to capture the essence of the danger posed by virtual weapons and cyber weapons are expanding the range of possible harm between war and peace, with significant consequences for national and international security. Kello's views are contradicted by Erik Gartzke, who contends that cyberwar has limited political utility, and that the Internet is generally an inferior substitute for terrestrial force in performing coercion or conquests.(Lindsay & Kello, 2014) This disagreement highlights the ongoing debate in cybersecurity studies regarding the true impact and effectiveness of cyber weapons. While Kello emphasizes the transformative nature of cyber weapons and their potential to reshape security

affairs, his argument has been criticized for its technological determinism and for overlooking the relevant scholarship in the field. The debate surrounding the impact of virtual weapons on international security remains ongoing, with scholars presenting different views on their significance and effectiveness in modern warfare.

A New Domain for Power Struggles

Realists view cyberspace as an extension of traditional domains of conflict (land, sea, air, and outer space). Cyberspace provides states with new opportunities for power projection and influence without physical confrontation. This includes cyber espionage, cyber warfare, and information operations aimed at undermining rivals(Choucri & Clark, 2013). Cyberspace has emerged as a new arena for power struggles between states, fundamentally altering the landscape of international relations. It is now considered a critical domain, alongside land, sea, air, and space and provides new opportunities for states to project power and influence globally, without traditional military force. States can engage in cyber espionage, cyber warfare, and information operations to undermine rivals and achieve strategic objectives.

Cyber operations allow states to exert influence covertly and with plausible deniability. This can include hacking critical infrastructure, stealing intellectual property, and manipulating information to sway public opinion or destabilize political systems. These activities are often less costly and risky than traditional military actions, making them attractive tools for statecraft.(Choucri & Clark, 2013) Cyberspace levels the playing field, allowing smaller or less powerful states and non-state actors to challenge more powerful ones. This asymmetry can destabilize traditional power hierarchies and introduce new dynamics into international relations. Smaller states can leverage cyber capabilities to punch above their weight, engaging in cyber-attacks that can cause significant damage to more powerful adversaries. Cyberspace is increasingly integrated with traditional military strategies. Cyber capabilities are used to complement physical military actions and provide a force-multiplier effect. For example, cyber-attacks can disrupt enemy communications, disable defense systems, and gather intelligence to support conventional military operations.(Isnarti, 2016)

Despite the competitive nature of cyberspace, there is growing recognition of the need for international cooperation to manage cyber threats. Efforts are underway to establish international norms and agreements that regulate state behavior in cyberspace, aiming to prevent escalation and promote stability(Stevens & Kavanagh, 2021). Cyberspace has become a significant arena for power struggles among nation-states by introducing new methods for projecting power and influencing international relations. The integration of cyber operations into state strategies, the development of cyber deterrence, and the establishment of international norms are all critical for navigating this new domain of conflict and cooperation.

Despite the borderless nature of cyberspace, realists emphasize the importance of state sovereignty and the need for states to control and secure their cyber infrastructure. The protection of national cyber boundaries is seen as crucial for maintaining sovereignty and preventing external interference.(Choucri, 2012) The concepts of sovereignty and territorial integrity in cyberspace have become increasingly complex as states navigate the challenges of governing and securing

their digital domains. Heinegg argued that the principle of territorial sovereignty applies to cyberspace, protecting cyberinfrastructure within a state's territory. States are prohibited from interfering with the cyber infrastructure of another state if the conduct is attributable and inflicts severe damage on the integrity or functionality of foreign cyberinfrastructure. This framework aligns cyber operations with traditional concepts of territorial sovereignty(Heinegg, 2012). Mueller challenges the application of traditional sovereignty to cyberspace, arguing that the unique characteristics of cyberspace, where territoriality and authority are separated, render traditional sovereignty concepts inappropriate. He suggests an alternative governance model based on the global commons, which may better address the challenges of cyberspace governance.(Mueller, 2020)

Some scholars explored the possibility of applying the territorial principle of sovereignty to cyberspace and contend that cyberspace should be included in the concept of "territory of the state" because of its role in social, economic, and political relations. This approach requires rethinking the spatial limits of state jurisdiction to include virtual spatial units that do not have a geographical extent (Terenteva, 2019). The interpretation of sovereignty in the context of cyber operations is still contested and evolving. While international law applies in cyberspace, there is still debate over when cyber operations constitute violations of sovereignty. The lack of consensus on applicable thresholds for such violations complicates the establishment of clear legal standards(Schmitt & Vihul, 2017). The implications of state sovereignty, the right to self-defense in cyberspace, the applicability of international law to cyberspace, the concept of territorial jurisdiction, and the conditions under which states can exercise the right of self-defense against cyber-attacks are important questions that are yet to be answered(Khanna, 2018). While states assert their sovereignty in cyberspace by creating national cyberspace zones, it involves the application of territorial notions of international law to persons, activities, and objects operating in cyberspace, reflecting the continued relevance of borders in the legal regulation of cyberspace.(Tsagourias, 2018) The principles of sovereignty and territorial integrity have been redefined in the context of cyberspace. Traditional concepts are being adapted to address the unique characteristics of the digital realm, with ongoing debates on how best to govern and secure cyberspace while respecting state sovereignty.

The limitations of realist theory in the context of cyberspace are significant and multifaceted, primarily because of the unique characteristics of the digital domain that challenge traditional realist assumptions about power, security, and state behavior. Realist theory traditionally emphasizes the state as the primary actor in international relations, focusing on military power and national interests. However, cyberspace has enabled non-state actors such as hackers, cybercriminals, and activist groups to play a pivotal role in international security dynamics. The emergence of these non-state actors complicates the realist framework, which often overlooks their influence and the implications of their actions in cyberspace. This shift necessitates a broader understanding of security, including a diverse array of actors beyond the state.(Taddeo, 2017)

Realism relies heavily on the deterrence theory, which posits that the threat of retaliation can prevent aggression. However, Taddeo pointed out that the nature of cyber operations

complicates traditional deterrence strategies. The anonymity and fluidity of cyberspace makes it difficult to attribute attacks to specific actors, undermining the effectiveness of deterrence. This lack of clarity can lead to miscalculations and escalations that are not adequately addressed by realist theory.(Taddeo, 2017) The uncertainty surrounding cyber operations poses a significant challenge to realist assumptions about military power and strategic stability. The inherent deficit of information about cyber operations creates gaps in the understanding of state behavior in cyberspace. This uncertainty complicates the realist focus on clear power dynamics and strategic signaling, as states may struggle to interpret the intentions behind cyber actions. (Gomez & Whyte, 2021)

The borderless nature of cyberspace challenges realist emphasis on territoriality and state sovereignty. The fluidity and anonymity of cyberspace have already disrupted the traditional concepts of national security and diplomacy. In this context, the ability of cyber actors to operate across borders undermines the realist notion of state control over their territory and complicates the enforcement of national laws. (Choucri, 2012)

Realist theory often simplifies conflicts into binary frameworks of war and peace, but the nature of cyber conflicts is more complex. While cybersecurity can be likened to traditional deterrents, the dynamics of cyber interactions require a more nuanced approach that incorporates elements from other theories, such as constructivism. This complexity challenges the realist framework, which may not fully account for the multifaceted nature of cyber conflicts and the interplay between various actors and interests(Watanabe, 2020). The application of existing international law to cyberspace is fraught with several challenges. The unique nature of cyberattacks complicates the application of traditional legal frameworks, making it difficult to determine when a cyberattack constitutes the use of force. This ambiguity further complicates the realist focus on deterrence and retaliation, as states may find it challenging to respond effectively to cyber threats when the aggressor's identity is obscured (Leng, 2023). The limitations of realist theory in the context of cyberspace are evident in its inability to adequately address the complexities introduced by non-state actors, challenges of deterrence, erosion of sovereignty, and ambiguous nature of cyber conflicts. As the digital landscape continues to evolve, these limitations necessitate a re-evaluation of traditional theories in international relations to better understand the dynamics of cybersecurity and its implications for global security.

Impact on the Traditional Concept of Security

The rise of cyberspace challenges the traditional realist concepts of security, which are based on territorial integrity and physical military capabilities. Realists now incorporate cyber capabilities into their analysis of state power and security, recognizing that cyber-attacks can disrupt critical infrastructure and undermine national security without physical invasion.(Isnarti, 2016) The impact of cyberspace on the traditional concepts of security is profound, reshaping how nations perceive and address security threats. The integration of cyberspace into national security strategies requires the continuous monitoring of technological developments and long-term strategic thinking to respond effectively to cyber threats.(Dobák, 2021) The unique characteristics of cyberspace, such as openness, heterogeneity, mobility, and dynamism, which necessitate new

security approaches. Traditional static security methods are inadequate for addressing novel threats like zero-day attacks and advanced persistent threats (APT), leading to the need for dynamic defense architectures and advanced security technologies.

Some scholars broadly categorize cyber risks into two dimensions: risks to cyberspace (threats to the infrastructure) and risks through cyberspace (threats facilitated by cyber technologies but targeting other domains). The complex nature of these risks requires international cooperation to manage effectively, though political differences often hinder such efforts.(Deibert & Rohozinski, 2010) In the first scenario cyberspace acts as an enabling medium and force multiplier if the cyber offensive operation is carried out by an otherwise weaker state or nonstate actor. The second scenario is where cyberspace itself is the target and offensive cyberoperations are launched to disrupt the entire ICT ecosystem of any state. Crippling Distributed Denial of Service (DDoS) attacks by Russia against Georgia and Estonia have shown how the entire ICT infrastructure can be lost to any organized and targeted campaign.

The importance of multilateral approaches to cybersecurity cannot be overlooked, given the transnational nature of cyber threats. International organizations like the Organization for Economic Co-operation and Development (OECD) play a crucial role in facilitating cooperation and developing global cybersecurity standards. Strategic thinking is essential for addressing the security challenges posed by cyberspace because tactical fixes do not last long in this fast-paced domain. They highlight the need for comprehensive cybersecurity strategies that integrate technological, political, and social dimensions to protect against cyber threats effectively. Cyberspace has become a critical domain for international power struggles, with major powers like the United States focusing on technological superiority to enhance their strategic capabilities. The integration of cyber strategies into national security policies reflects the growing importance of cyberspace in maintaining global power balance.

Conclusion

Cyberspace as a domain challenges traditional international relations theories, which are based on state-centric models and territorial sovereignty by introducing new forms of conflict and cooperation, necessitating a reevaluation of how states interact in the global arena. The impact of cyberspace on the traditional concepts of security is profound, requiring new approaches to national and international security. The unique characteristics of cyberspace, such as its borderless nature and rapid technological advancements, necessitate dynamic defense strategies, international cooperation, and a re-evaluation of traditional security frameworks to address the complex challenges posed by cyber threats.

References

Arquilla, J., Ronfeldt, D., Toffler, A., & Toffler, H. (1997). CYBERWAR IS COMING! In J. Arquilla & D. Ronfeldt (Eds.), *In Athena's Camp* (1st ed., pp. 23–60). RAND Corporation; JSTOR. http://www.jstor.org/stable/10.7249/mr880osd-rc.7

Choucri, N. (2012). *Cyberpolitics in International Relations*. https://doi.org/10.7551/mitpress/7736.001.0001

Choucri, N., & Clark, D. (2013). Who controls cyberspace? *Bulletin of the Atomic Scientists*, *69*, 21–31. https://doi.org/10.1177/0096340213501370

Choucri, N., & Clark, D. D. (2019). *International relations in the cyber age*. https://doi.org/10.7551/mitpress/11334.001.0001

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, *68*(2), 70–77. https://doi.org/10.1177/0096340212438696

Cranor, L. F., & Garfinkel, S. (2005). *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly Media, Inc.

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*, 15–32. https://doi.org/10.1111/J.1749-5687.2009.00088.X

Dobák, I. (2021). Thoughts on the evolution of national security in cyberspace. *Security and Defence Quarterly*, *33*(1), 75–85. https://doi.org/10.35467/sdq/133154

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, *45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Gomez, M. A., & Whyte, C. (2021). *Unpacking strategic behavior in cyberspace: A schema-driven approach*. https://doi.org/10.31235/osf.io/hfsru

Heinegg, W. H. V. (2012). Legal implications of territorial sovereignty in cyberspace. *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–13.

Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. *The Journal of International Studies*, *5*, 151–165. https://doi.org/10.25077/AJIS.5.2.151-165.2016

Kapell, M. W., & Elliott, A. B. R. (2013). *Playing with the Past: Digital Games and the Simulation of History*. Bloomsbury Publishing USA.

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War*. Simon and Schuster.

Khanna, P. (2018). STATE SOVEREIGNTY AND SELF-DEFENCE IN CYBERSPACE. *BRICS Law Journal*. https://doi.org/10.21684/2412-2343-2018-5-4-139-154

Kour, R., Al-Jumaili, M., Karim, R., & Tretten, P. (2019). eMaintenance in railways: Issues and challenges in cybersecurity. *Proceedings of the Institution of Mechanical Engineers Part F Journal of Rail and Rapid Transit*. https://doi.org/10.1177/0954409718822915

Kozub, M., & Mitręga, A. (2021). Strategic Thinking about Security in Cyberspace. *Rocznik Bezpieczeństwa Morskiego*, *XV-Wydanie specjalne*, 1–28.

https://doi.org/10.5604/01.3001.0015.5893

Leng, Y. (2023). When can cyberattack constitute use of force: A case study of cyberattack in the russia-ukraine conflict. *Lecture Notes in Education Psychology and Public Media*. https://doi.org/10.54254/2753-7048/17/20231249

Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information and Computer Security*. https://doi.org/10.1108/ics-04-2020-0054

Lindsay, J. R., & Kello, L. (2014). Correspondence: A cyber disagreement. *International Security.* https://doi.org/10.1162/isec_c_00169

Mueller, M. L. (2020). Against Sovereignty in Cyberspace. *International Studies Review*. https://doi.org/10.1093/isr/viz044

Schmitt, M., & Vihul, L. (2017). Respect for Sovereignty in Cyberspace. *Texas Law Review*, *95*. https://consensus.app/papers/sovereignty-cyberspace-schmitt/7136cd4013045845b02671049d2387fd/

Stevens, T., & Kavanagh, C. (2021). Cyber Power in International Relations. *The Oxford Handbook of Cyber Security*. https://doi.org/10.1093/oxfordhb/9780198800682.013.4

Taddeo, M. (2017). The limits of deterrence theory in cyberspace. *Philosophy & Technology*. https://doi.org/10.1007/s13347-017-0290-2

Terenteva, L. V. (2019). Territorial Aspect of State Jurisdiction and Sovereignty in Cyberspace. *Lex Russica*. https://doi.org/10.17803/1729-5920.2019.149.4.139-150

Tsagourias, N. (2018). Law, Borders and the Territorialisation of Cyberspace. *Indonesian Journal of International Law*, *15*. https://doi.org/10.2139/SSRN.3213511

Watanabe, S. (2020). *States' capacity building for cybersecurity: An IR approach*. https://doi.org/10.1007/978-3-030-62803-1_18