

Cybersecurity as an Emerging Dimension in Security Studies in the digital age الأمن السيبراني كبعد جديد في الدراسات الأمنية في العصر الرقمي

Sahki Samar *, Algeria Shield Laboratory
for Comprehensive Security and Strategic
Studies, Blida 2 University, Algeria.
s.sahki@univ-blida.dz

Received: 29/10/2025

Accepted: 22/11/2025

Abstract:

The advancement of Artificial Intelligence has brought significant technological transformations to the field of International Relations, particularly within security studies. This is evident in the emergence of new concepts such as cybersecurity, cyberspace, and cyber warfare, which have reshaped the forms and patterns of interactions among international actors. These developments call for a redefinition of core concepts like security and power, challenging traditional analytical frameworks. This study explores the implications of cyber transformations on the theorization in security studies, concluding that most existing theories remain confined within a narrow military understanding of security. This highlights the need for broader and more comprehensive approaches capable of addressing this rapidly evolving and complex reality.

Keywords: Cyber space; Cybersecurity; Security studies; IR, Cyber threats, Critical Approaches.

ملخص:

لقد أدى التطور في التكنولوجيا في العصر "الذكاء الاصطناعي" إلى إحداث مجموعة من التحولات في حقل العلاقات الدولية بشكل عام والدراسات الأمنية بشكل خاص، خصوصاً مع بروز مفاهيم جديدة كالأمن السيبراني، الفضاء السيبراني والحروب السيبرانية. الأمر الذي أثر على شكل وأنماط التفاعلات من جهة، وكذا

* corresponding author

على أدوار الفواعل الدولية من جهة أخرى، وأصبح يستدعي إعادة تعريف الأمن والسيادة وغيرها من المفاهيم التي تشكل حجر الأساس لهذا الحقل.

حاولنا في إطار دراستنا التركيز على تداعيات التحولات السيبرانية على التنظير في حقل العلاقات الدولية والدراسات الأمنية، واختبار مدى قدرة نظريات العلاقات الدولية على مواكبة، فهم وتفسير هذه المفاهيم الجديدة وتداعياتها على أمن وسيادة الدول القومية. في الأخير توصلنا إلى نتيجة مفادها عدم قدرة أغلب نظريات العلاقات الدولية الخروج من قالب الأمن والعسكري الضيق للأمن، الأمر الذي يستدعي فهما أوسع وأكثر شمولاً للأمن والسعي إلى تبني مقاربات نقدية قادرة على مواكبة هذا الواقع المعقد في المستقبل.

الكلمات المفتاحية: الفضاء السيبراني؛ الأمن السيبراني؛ الدراسات الأمنية؛ العلاقات الدولية؛ التهديدات السيبرانية.

Introduction:

Security studies have traditionally been closely associated with the military dimension of power, deterrence, and the protection of the state. Barry Buzan, one of the leading scholars of the Copenhagen School of Security Studies, went beyond this conventional military focus by expanding the concept of security into five key dimensions, known as the “Sectors of Security.” However, even with these conceptual expansions, contemporary global transformations—including rapid technological advancements, the rise of borderless cyberspace, and the emergence of invisible and asymmetric threats—remain inadequately addressed.

In this context, the concept of cyberspace and its relevance to international relations has gained increasing importance. Cyberspace now extends far beyond the traditional technical domain of protecting information systems and technology; it encompasses significant political and strategic dimensions due to its profound impact on the understanding of security in the twenty-first century. Despite its growing significance, cyberspace has received limited attention from scholars of international relations. This underscores the urgent need to develop new conceptual and theoretical frameworks that align with the evolving nature of contemporary cyber activities.

Accordingly, the core problem driving this study: Is the field of security studies capable of absorbing the rapid technological changes of the digital age and the resulting transnational cyber threats?

We have used Descriptive–Analytical Approach which can be effectively employed by first describing the evolution of the concept of

cyber security and the transition from traditional, state-centered military perspectives to broader, technology-driven approaches influenced by cyberspace. The analytical aspect of this method then allows the researcher to critically examine how these transformations challenge existing security theories, identify gaps in traditional frameworks, and evaluate emerging theoretical propositions that better capture the complexity of cyber interactions.

Comparative Method: to compare how different IR/security theories (Realism, Liberalism, Constructivism, Critical Theory, Copenhagen School) address or fail to address: Cyber threats and this helps us to expose theoretical gaps and justify the need for new frameworks.

The aim of this study primarily proposes a conceptual framework—the cyberspace structural modifier—while also critically reviewing existing literature. It combines theoretical innovation with a synthesis of empirical observations to clarify how cyberspace reshapes international relations.

First: Conceptual framework of cybersecurity

This section serves as a conceptual introduction to cybersecurity and an attempt to approach the concept from the perspective of international relations.

Firstly, it is necessary to distinguish between the many overlapping terms like cyberspace, cyber politics and cybersecurity and then attempt to link this concept to the field of international relations, and more specifically, to the field of security studies.

1.Cyberspace:

The historical and philosophical roots of the term "cyber" are often considered to lie in Plato's allegory of the cave in the Republic. In the twentieth century its semantic identity was derived from the term "cybernetics" the study of communication and control rendered famous by Norbert Wiener in *Cybernetics: Or Control and Communication in the Animal and the Machine* in 1948 (Krieger,2013, p.267).

Until recently, cyberspace was considered largely a matter of low politics—background conditions and routine decisions and processes. In recent years, issues connected to cyberspace and its uses have catapulted into the highest of high politics. A newly coined term, "cyber politics," refers to the conjunction of two processes: those pertaining to politics surrounding the determination of who gets what, when, and how, and those enabled by the uses of cyberspace, a new arena of virtual interactions (Krieger,2013, p.267).

Military strategists in the United States and the west started to think about the importance of networked computers for war fighting. During the 1990s, militaries began to treat cyberspace as “domain of warfare” in theory and practice. By 2011, the Pentagon had officially added cyberspace as the so-called “fifth” domain of warfare, next to land, sea, air, and space. From early on, this particular debate was characterized by the double-edged sword perspective mentioned already: strategists saw great opportunities for winning wars through technology-aided “information dominance,” but at the same time they anticipated growing security- relevant vulnerabilities due to increasing dependencies on computers (Lacy and Prince, 2018, p p.11-12).

Cyberspace is understood as a multifaceted domain composed of three core dimensions. The first is the material dimension, which includes the physical infrastructure of information technology such as networks, devices, and satellites. The second is the ideational dimension, involving the norms, rules, and behavioral expectations that govern how this infrastructure is used. The third is the semantic dimension, centered on the information and data transmitted through digital interactions. Together, these dimensions shape actors’ behavior in cyberspace and influence power dynamics by granting strategic advantages to those with greater technological and economic capabilities. Moreover, disruptions to the physical layer can directly impair information flows and digital communication, highlighting the interdependence and unique nature of cyberspace within international relations (Foulon, M., & Meibauer, G, 2024, p.430).

2.Cyber politics:

There is, as yet, no decisive description of cyber politics; we can say that with the creation of cyberspace, a new arena for the conduct of politics is taking shape, and we may well be witnessing a new form of politics.

Cyber politics, is a recently coined term, refers to the conjunction of two processes or realities — those pertaining to human interactions (politics) surrounding the determination of who gets what, when, and how, and those enabled by the uses of a virtual space (cyber) as a new arena of contention with its own modalities and realities. Despite differences in perspectives worldwide, there is a general scholarly understanding of the meaning of “politics.” It is the complexity attending the prefix cyber that distinguishes this newly constructed semantic (Nazli, 2013, p.5).

We can say that, Cyber politics is the integration of politics and technology. It affects not only the politicians who choose to employ it

in their platforms, but also individual citizens who are responsible for electing these politicians (SOMA, n.d, pp.2-4).

3.Cyber security:

is academically defined as the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights (Etschmaier, 2019, p.141).

Cyber security is the set of security measures that can be taken to protect the cyberspace and user assets against unauthorized access and attacks. It is clear from this point of view that there is every tendency for the cyber criminals to attack any data base that contains a vital information that can lead to exposure of that particular database (Eze1 and others, 2023, p.13).

The importance of cyber security as an emerging issue in International Relations cannot be overstated; what can be overstated is the novelty of the domain. There is a long history of speculation on the role of digital technology in security studies. To some extent originating with Arquilla and Ronfeldt's concept of net war and cyber war, there has been an extensive history of theoretical and ethical examinations regarding cyber security concerns. The problem with these past examinations is that they often rely on old frameworks to examine new methods of interaction. Scholarly viewpoints on the cyber security debate tend to be dominated by the popular media's concern with the possibility of global catastrophe brought on by our reliance on technology. The focus has been on the consequences of the technology without first understanding the domain, its coercive potential, and usage by actors (Valeriano and Maness, p.259).

Accordingly, it is evident that there is no clear and precise definition of cybersecurity as a concept or term within the field of international relations or as a sub-discipline in security studies.

It can be said that the new challenges posed by artificial intelligence in the digital age to the field of international relations in general and security studies in particular now require us as researchers to reconsider expanding the dimensions of security to include technological and digital challenges.

Second: Cybersecurity in International Relations Theories

The issue of cybersecurity and the risks that technology brings to the security and sovereignty of states have not been a main focus in

most theories of international relations.

However, as Steve Smith mentions, when we look at these theories through the lens of cybersecurity, we find that the majority of international relations theories focus on traditional aspects of security and don't pay much attention to the cyber aspect or the new dangers that come from advanced technology in the digital age. This section will explore these ideas in more detail.

1. Realism and Neo-realism

Stephen Walt from the Kennedy School wants to set clear boundaries and support a more objective analysis. In his 1991 work, Walt argues that security studies should focus on "the phenomenon of war," especially war carried out by military forces under the control of state actors. He also includes other related issues such as arms control and crisis management, because they affect the chances and types of war that might happen. Neorealists argue against including cybersecurity in the study of security, saying that the real-world impact of cyberattacks on a state's physical security and military strength is still not fully understood (Cavelty, 2007; Kelly & Fitzgerald, 2009; Libicki, 2009, p.10).

According to James Adams, cyberspace creates a new kind of security dilemma for all states because it brings a lot of uncertainty. In his article "Virtual Defense" in Foreign Affairs, he uses a strict neorealist view to talk about cyberterrorism and cybersecurity. He sees the Internet as an anarchic system, saying that "cyberspace has become a new international battlefield." Since there is no global governing authority, the Internet easily fits into the realist model of security. Each state is on its own or with allies it can't fully trust, trying to build up its cyber capabilities and defenses while fearing that any move or leak by another state could directly threaten its own security. Both offensive and defensive realists talk about the idea of first strike capability as a way to end a security dilemma and make sure an enemy cannot retaliate. Unfortunately, in cyber warfare, it is nearly impossible to see or predict an incoming attack. And because the Internet is global and constantly changing, a state can never hope to cut off another state and stop an enemy from launching a cyber counterattack (Petallides, 2012).

2. Copenhagen School and the Danish institute of security studies

Ole Waever and Barry Buzan's vision for security studies includes a far more comprehensive and in-depth agenda. They draw attention to the possibility of economic, sociological, and environmental challenges to national security while simultaneously

recognizing military and political actors as sources of security threats. Furthermore, the referent object of security may be a person or a global actor, such as a state, a corporation, a nation, or a society. According to this viewpoint, even in cases where the actor is an individual and the existential danger is economic devastation, cyberthreats obviously meet the criteria for security concerns for referent objects. States have previously determined that cybersecurity is a part of national security, as can be seen within this framework. We must take into account how these challenges affect national security and many scholars in the field as long as state leaders securitize cyber dangers in speeches and policy proposals. In their 1996 attempt to bring disparate scholarly viewpoints together, Krause and Williams contended that even if we concentrate on emergency state responses, we also need to comprehend the "why" underlying securitization. Understanding the security viewpoints of non-governmental stakeholders and the dangers posed by non-state actors—a dynamic that also pertains to cybersecurity—is frequently necessary to answer the "why." Malicious capabilities in cyberspace are not monopolized by nation-states, as many academics have argued. Furthermore, because of how quickly things happen and how interconnected we are, the cyber threat can spread quickly across all security levels. Returning to neorealism, states continue to be the actors with the authority and power to fortify defenses against the majority of existential cyberthreats, which means they continue to play a crucial role in resolving cyberthreats to national security. Although private sector actors play a significant role in cybersecurity in the majority of nations, Krause and Williams (1996) pointed out that "security cannot exist in the absence of authority." (Forest, 2010, pp.211-225).

3.Securitization theory:

Since cybersecurity is frequently left to technical considerations, it is crucial to start by situating it within the larger framework of national security challenges. In his paper "The Cyber Threat to National Security: Why Can't We Agree?" Hare, Forrest makes the case that cyberthreats ought to be regarded as national security issues, necessitating their examination within the theoretical frameworks of security studies. By evaluating the securitization process and the ways in which different stakeholders have securitized cyber hazards, Forrest places cybersecurity within the broader field of security studies. By showing that cyber threats can be considered national security issues, he makes it suitable to use security studies theories, especially Buzan's framework.

In his seminal paper "National Security as an Ambiguous Symbol" (Wolfers, 1952, pp. 481–502), Arnold Wolfers highlighted that determining whether a threat qualifies as a national security issue and the actions that follow are essentially political choices rather than legal or technological ones. In 1997, almost fifty years later, Buzan and his associates investigated further what they called "securitization," the process by which political agendas are elevated to the level of security (Buzan, 1997, p. 25). To put it another way, a problem is securitized when it is framed as an existential threat (usually to the entire nation-state) that calls for drastic measures (beyond the bounds of normal political processes). Therefore, the victim, the threat, and the victim's comprehension of the threat are all essential elements of the process.

Criminals, hackers, terrorists, and nation-states are examples of threat agents in cyberspace. Threats from separatist movements or the fall of the regime could be considered existential threats when the state and its institutions are the victim. Since national defense is regarded as a public good, public action may be warranted when individuals confront existential risks to their well-being, either directly or through the loss of state institutions. Because they are responsible for representing the interests of their constituents, politicians are therefore motivated to securitize risks to individual residents. In the end, different stakeholders in cyberspace may face different possible hazards. It is evident that a variety of securitization attempts may result from the vast range of threat agents and the broader assessment of possible victims.

The academic dispute over the extent of national security with in the area of security studies is further fueled by the ambiguous character of national security in cyberspace (Forrest, 2010, pp.211-225).

cybersecurity was "securitized" by many governments in the West and national security agencies obtained considerable power in this emergent domain. Cyberattacks were framed in the discourse of political leaders during this period as an existential threat to nations that would cause major disruptions to national economies and be catalysts for conflict between the great powers. Growing concerns over internet failure and instability and attacks against critical infrastructure were instrumental in creating fear and paranoia, but also served the political and commercial purposes of securitizing actors and hindered the emergence of societal approaches. Later in the period, owing partly to the growing influence of social media platforms, the societal effects of disinformation were layered into anxiety-saturated cyber policy.

Crucially, these cases also led to path dependencies that deteriorated the government-society relationship and caused military

agencies and structures to take measures that exacerbated cybersecurity and societal issues. (Burton and Lain, 2020, PP.452-453,).

4.The Constructivist and Neoliberal Viewpoint

Eriksson and Giacomello emphasize the value of collaboration in their paper "The Information Revolution, Security, and International Relations" in order to lessen the threat of cyberattacks. Although they stress that "government alone cannot secure cyberspace," they offer no practical substitute. According to neoliberalism, the establishment of multinational organizations may be able to address this security conundrum. A worldwide body made up of both states and non-state entities dedicated to maintaining cyber security would significantly reduce the uncertainty that each state currently faces, even though it would be challenging to start.

Eriksson and Giacomello view "symbolic politics as very relevant for understanding digital age security," as the constructivist school places a strong emphasis on the significance of ideas, symbols, and their meaning. Although it is a tool for information transmission, the Internet is a special medium that has taken on a life of its own and is always changing (Petallides, n.d,2012).

5.Cybersecurity in Feminism and Critical Theories

State-centric, military, and unduly securitized viewpoints are frequently highlighted in current international relations study on cybersecurity. Nonetheless, a growing corpus of feminist and critical scholarship aims to subvert this prevailing viewpoint. Basu and Biddolph suggest queering cybersecurity as a creative initiative. through engaging critical cyber scholarship with queer scholarship, methods, and possibilities. Technical viewpoints that are primarily concerned with threats and vulnerabilities have long dominated cybersecurity scholarship, generally ignoring the social dynamics and human environment in which cybersecurity functions. But more recently, a growing corpus of feminist and critical scholarship has emerged both inside and outside of International Relations (IR) to question prevailing militaristic views of cybersecurity (Basu & Biddolph, 2025, pp.1-2).

Third: Rethinking Cybersecurity Theories

Within this section, we will explore a new perspective on cybersecurity. This approach suggests moving beyond the narrow view of traditional security and deconstructing the concept of securitization as applied to cybersecurity. a perspective that we will examine in detail in this section.

If securitization is a process driven by ontological insecurity, defined here as an erosion of identity and an anxiety created and fuelled by globalization, then the place to start in a process of cyber-securitization must be to reframe discourse and present cyber ‘threats’ in less apocalyptic, fearful tones. This involves moving towards a normalized and less polemic political debate in which cybersecurity is not continually treated as an emergency but rather as a regular feature of modern political interactions (Burton and Lain ,2020, P.461).

Joe Burton & Clare Lain in their study propose a move towards a societal security-based approach to cyber theory and policy. they argue that the societal security concept, which first emerged in the aftermath of the Cold War, is a better theoretical fit for cybersecurity concerns than traditional national security models, and that much of the malicious cyber activity over the last decade, including cyberespionage, cyber coercion, cyber and information warfare, and the subversion of social media, has been targeted at, and caused by, societal tensions. Focusing on societal cybersecurity, will help sectors where much of the impact of cyberattacks lies, including in health, energy, transport, finance and democratic governance and will help to enhance societal resilience against cyberattacks (Burton and Lain ,2020, P.450).

It is worth noting that what is referred to in the literature of Western theoretical studies as Queer Studies or Queer Theory is a critical approach that seeks to redefine the traditional ideas on which international relations theories are based—such as the concepts of identity, security, power, or authority. This is done by rethinking these conventional concepts in a critical manner that aims to understand why certain groups or minorities are excluded from security debates. Accordingly, proponents of this perspective seek to deconstruct all traditional concepts and reject, in their view, all classical classifications that distinguish between identities or socio-cultural categories such as male and female.

Accordingly, Joe Burton & Clare Lain attempted to reconsider the concept of cybersecurity from a queer perspective in order to move it beyond its traditional understanding.

Fourth: cyberspace as a structural Factor in International Relations

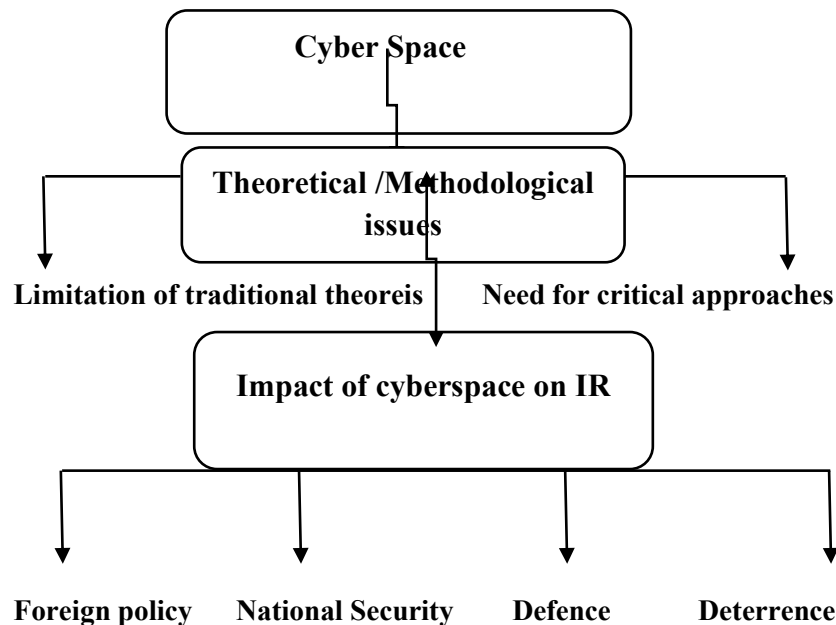
Ever since cyber security issues have appeared on the agenda of national and international politics, Jon R. Lindsay argues on the ambiguity of a cryptologic advantage, two analytically distinct perspectives have informed the debate about their relevance for cyber security politics. A first perspective builds on the premise that technology determines politics. Anticipating the transformative

potential of emerging technologies, this view tends to extrapolate dramatic consequence for security politics. A second perspective starts from the opposite end of the relationship and assumes that politics determines technology. Such an analytical perspective translates into expectations that the sociopolitical context mitigates the supposed advantages of cyber offense and reinforces established power relationships (Cavelty, 2022, p. 246).

Foulon, M., & Meibauer, G. suggests that Cyberspace can be considered a structural factor influencing international relations, as it has system-wide effects and shapes the behavior of all states. It not only adds to or diminishes a state's material capabilities but also alters the nature and intensity of interactions between states and non-state actors, affects incentives for offensive and defensive behavior, and can empower smaller states while accelerating conflict dynamics. Although cyberspace originated in a limited number of states, its nature and effects transcend the boundaries of any single state, and its impact cannot be explained solely by the capabilities of one state, making it a fundamental systemic element for understanding contemporary international relations.

Cyberspace acts as a structural modifier in international relations by shaping key areas such as deterrence, for example Russia's 2016 interference in the US elections exposed the inability of traditional deterrence theory to account for unattributed, asymmetric cyber influence. We have also the area of foreign policy, uncertainty, and state-non-state interactions. It complicates conventional deterrence by enabling persistent, unattributed cyber actions, altering cost-benefit calculations, and influencing alliance dynamics. In foreign policy, cyberspace affects decision-makers' choices by introducing uncertainty, requiring specialized capabilities, and creating new opportunities for diplomacy and status-seeking. It modifies uncertainty by expanding information availability while also generating risks from overload and misinterpretation. Finally, cyberspace blurs boundaries between states and non-state actors, empowering a wider range of actors, including hackers, corporations, and insurgent groups, and reshaping interactions, conflict dynamics, and the exercise of power in the international system (Foulon, M., & Meibauer, G, 2024, p. 440-447).

Figure N.1: illustrating the intersection between Cyberspace and IR.



Source: Diagram prepared by the researcher.

From the diagram above, we conclude that cyberspace has triggered a transformation in the structure of international relations by redistributing power, altering the concept of deterrence, and diversifying foreign policy tools. The question arises: have International Relations theories been able to accommodate these new changes imposed by this dimension? We conclude that most International Relations theories remain largely confined to the narrow military dimension. Accordingly, there is an urgent need to improve the responses of IR theories and to balance traditional and contemporary concepts within the field.

CONCLUSION

It could be said that the traditional approaches to international relations have not understood the nature of emerging cyber threats in the age of artificial intelligence. In particular, classical theories such as realism have tended to center their attention on the state as the principal actor in IR while ignoring threats from non-state individuals or groups as well as cyberspace.

Furthermore, all forms of realism associate's security with military power and considers tangible threats, thereby concentrating on the material and military aspects of security. In contrast, cyber threats

are not only opaque but are also non-material and transborder, and therefore, elusive to traditional security paradigms.

Even though IR critical theories have sought to address the politics of security threats, and redefined concepts like identity, power and sovereignty, the urgent requirement is to reconceptualize security in more holistic terms that address the technical, social and politics of cyber threats. Accordingly, we arrive at the following results :

1. Traditional security theories are no longer sufficient to explain cyber threats. Despite the expansion introduced by the Copenhagen School, most classical theories—especially Realism and Neorealism—remain anchored in a military-centric understanding of security.
2. cyber threats have expanded the referent object of security. Security is no longer limited to the state, this confirms the need for broader, more inclusive understandings of security.
3. Security studies must incorporate new concepts or risk losing relevance. The study concludes that the field needs: new definitions of security and sovereignty, theoretical models that account for non-state actors and digital interdependence, and frameworks capable of explaining cyber coercion, hybrid warfare, and AI-enabled threats. Without theoretical evolution, security studies will remain stuck in a pre-digital paradigm.

Bibliography List

A/ Books:

- Buzan, B., Wæver, O., & de Wilde, J. (1997). *Security: A new framework for analysis*. Lynne Rienner.
- Dunn Cavelty, M., & Wenger, A. (2022). *Conclusion: The ambiguity of cyber security politics in the context of multidimensional uncertainty*. ETH Library.
- Krieger, J. (Ed.). (2013). *The Oxford companion to comparative politics*. Oxford University Press.
- Valeriano, B., & Maness, R. C. (2023). International relations theory and cybersecurity: Threat, conflict, and ethics in an emergent domain. In C. Brown & R. Eckersley (Eds.), *The Oxford handbook of international political theory*. Oxford University Press.

– B/Articles and reviews

- Basu, S., & Biddolph, C. (2025). Queering cybersecurity: An alternative research agenda. *Critical Studies on Security*, 13(2).

- Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: Towards a societal approach. *Journal of Cyber Policy*, 5(3).
 - Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 40(1).
 - Etschmaier, M. M. (2019). Critical issues of cybersecurity: Solutions beyond the technical. *International Journal of Computer Applications (IJCA)*, 26(4).
 - Foulon, M., & Meibauer, G. (2024). *How cyberspace affects international relations: The promise of structural modifiers*. *Contemporary Security Policy*, 45(3).
 - Eze, V. H. U., Ugwu, C. N., & Ugwuanyi, I. C. (2023). A study of cyber security threats, challenges in different fields and its prospective solutions: A review. *INOSR Scientific Research*, 9(1).
 - Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, 8(1).
 - Saida Brahmi,” Artificial Intelligence Applications and Family Communication Dynamics in the Arab World”, *Social Sciences and Humans Review*, vol.17, NO 2. 2024, p.427.
 - Wolfers, A. (1952). National security as an ambiguous symbol. *Political Science Quarterly*, 67(4).
 - C/Web Articles / Reports:
 - Choucri, N. (2013). Cyberpolitics in international relations. *MIT Center for International Studies Magazine*, Spring 2013.
 - Hare, F. (2010). The cyber threat to national security: Why can't we agree? In *Conference on Cyber Conflict*, NATO CCD COE, Tallinn.
 - Mazurier, P. (n.d.). *Introduction to cyber politics*. Retrieved from http://www.cyberpolitics.eu/cyberpolitics_art_02_cyberpolitics.html
 - Petallides, Constantine J. (2012). "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat." *Inquiries Journal/Student Pulse*, VOL. 4 NO. 03 RETRIEVED from <http://www.inquiriesjournal.com/a?id=627>
 - Schiliro, F. (2022). *Towards a contemporary definition of cybersecurity*. Australian Defence Force Academy, University of New South Wales, Macquarie University.
- SOMA. (n.d.). Special political and decolonization – Cyberpolitics and globalization. *Southern Ontario Model United Nations Assembly*.