Strategic Discourse Quarterly
Vol II. No V. Summer 2025
Pages 133-173

The Impact of Emerging Cyber Technologies on National Security

Abdolreza Taraghi[1], Abolhasan Firouzabadi[2], Ali Asghar Behnamnia[3], Mohammad Reza Karimi Ghahrudi[4]

Receipt Date: 2025/07/20 Date of Acceptance: 2025/08/06

Abstract

The impact of emerging cyber technologies on national security and the rapid and profound developments in cyber technologies, which exert strategic influences on sovereignty in various social, cultural, economic, political, technological, security, and military-defensive dimensions, necessitate a comprehensive, structured, and cohesive approach to safeguard national interests. This is aimed at raising awareness of ongoing transformations to enable timely decision-making and planning for the country's managers.Therefore, the importance and necessity of identifying the type and extent of the comprehensive impacts of emerging cyber technologies on national security is essential for the purpose of leveraging the opportunities ahead and timely countering potential threats in the framework of scientific research. This study aims to extract the specific and abstract characteristics of emerging cyber technologies as a unified entity, with the goal of uniquely identifying them as a singular existence, so that, in the next step, the impacts of each of these characteristics on various dimensions of national security can be examined to achieve the desired outcome.the research was conducted using a mixed-methods approach, and the necessary information was gathered through documentary and library methods, employing a researcher-developed questionnaire. The data was analyzed using descriptive and inferential methods with the aid of SPSS 23 software. As a result of the analysis and synthesis of the relationships between the variables based on the presented results, it can be stated that, in the first rank, the component of "data-driven intelligence" has the strongest direct and positive relationship with national security. In the second rank, "complexity and change in the environment" is positioned, followed by "convergence and immersion" in the third rank. Ultimately, it was demonstrated that all dimensions of national security are significantly and directly influenced, with the "political-security" dimension exhibiting the highest level of impact.Keywords.

Keywords: Cyber Space, Emerging Technologies, National Security, Technology Characteristics, Technology Convergence.

[1]PhD Student, National Defense University (Corresponding Author),
Email: taraghi@borhanid.com
[2] Instructor, National Defense University, Email: Alhasanfirouzabadi@gmail.com
[3] Faculty Member, Islamic Research Center of the Islamic Consultative
[4] Faculty Member, Malek Ashtar University of Technology, Email: m.karimi@sndu.ac.ir

Introduction and Problem Statement

The impact of cyberspace on all aspects of life, considering the emergence of complexities and chaotic conditions in today's era due to the rapid changes in the environmental conditions arising from strategic influencing factors with high granularity, depth, and diversity, necessitates the awareness of high-level decision-makers regarding the effects of emerging technological trends. Given the increasing intertwining of influential factors in cyberspace and the diversity of their strategic impacts, enhancing awareness and capability among decision-makers to understand the environment is essential for effective scene management, and without it, strategic surprises are certain to occur. Maintaining readiness and establishing deterrence against new threats, as well as leveraging emerging opportunities and capabilities from a broad security perspective, are crucial for advancing the lofty goals of the Islamic system on a global scale. Cyber technologies serve as one of the foundational variables in the phenomenon of security, contributing to endogenous power and national cohesion in the digital age. Emerging technologies, due to their rapid growth and influential power in transforming environmental conditions, are referred to as Exponential Technologies, Disruptive Technologies, Black Swan phenomena, boundary-breaking, and enabling technologies, despite the semantic and maturity level differences in their definitions within scientific documents. Inherently, technology is the primary factor in the emergence and transformative growth of cyberspace, and it is, in fact, the expansion of cyber technologies that leads to strategically deep impacts at both national and transnational levels across various dimensions of human life, which continue to increase in scope, diversity, and complexity.

In light of this rapid, profound, and complex growth and development of cyberspace, a significant portion of the assets of individuals, organizations, and countries is consumed for the material and spiritual acquisitions of citizens. This intertwining of various aspects of life with cyberspace means that any instability, insecurity, or challenge in this domain directly affects the lives of individuals, public and social security, and ultimately national security. Further examples of these impacts in various dimensions will be discussed. From a political perspective, in leveraging empowering technologies, one can refer to the strategy of "coercive power" (Billingsley, 2023; Gompert, Binnendijk, 2016) employed by the United States against Iran, utilizing cyber technologies as

a powerful tool for political bargaining in shaping international relations and the realm of cyber diplomacy, which is considered a manifestation of cyber power. The topic of cyber power, due to its deep penetration and the inherently comprehensive nature of cyberspace across all strategic domains of the country, possesses all the characteristics of national power and is regarded as an important tool for enhancing national security in order to protect national interests and values (Helili et al., 2018).

In light of this rapid, profound, and complex growth and development of cyberspace, a significant portion of the assets of individuals, organizations, and countries is consumed for the material and spiritual acquisitions of citizens. This intertwining of various aspects of life with cyberspace means that any instability, insecurity, or challenge in this domain directly affects the lives of individuals, public and social security, and ultimately national security. Further examples of these impacts in various dimensions will be discussed. From a political perspective, in leveraging empowering technologies, one can refer to the strategy of "coercive power" (Billingsley, 2023; Gumpert and Bindedjik, 2016) employed by the United States against Iran, utilizing cyber technologies as a powerful tool for political bargaining in shaping international relations and the realm of cyber diplomacy, which is considered a manifestation of cyber power. The topic of cyber power, due to its deep penetration and the inherently comprehensive nature of cyberspace across all strategic domains of the country, possesses all the characteristics of national power and is regarded as an important tool for enhancing national security in order to protect national interests and values (Helili et al., 2018).

Cyber power, in coordination with other forms of national power, operates within a harmonized ecosystem in constant interaction and is one of the significant factors influencing the changing geometry of the new world order. From a legal perspective, due to the emergence of new concepts such as smart contracts and the role of non-human autonomous agents in economic, social, security, and defense domains, the damages resulting from perceptual delays and lagging in proactive policymaking and legislative actions at both the national level and within contemporary international organizations is clearly evident.

From a socio-cultural perspective, in the absence of digital media literacy among both the general public and elites, we are confronted with the cognitive warfare of the enemy, particularly through the use of autonomous software agents based on deep learning methods in social

networks. Unfortunately, this leads to the audience's susceptibility to changes in viewpoint, attitude, worldview, and interpretation, in such a way that shaping the identity characteristics and perceptions of users (taste-making) and diverting them towards a predetermined desirable outcome has become the target.

Today, there exists an opportunity for coordinated proactive action in leveraging this capacity for the production and widespread dissemination of high-quality content aligned with revolutionary values. From a defense perspective, the development of fourth and even fifth-generation military weapons based on emerging cyber technologies has transformed the nature of military offense and defense. With the emergence of hybrid warfare and smart attacks and defenses in cyberspace, the topics of monitoring, surveillance, and defense have undergone significant transformation, challenging the nature of command and control from the perspective of measurement and autonomous action with a paradigm shift in meaning. Economically, the development of the digital economy, gig economy, freelance commerce, modern banking, digital currency, and cryptocurrencies has created an unprecedented landscape of opportunities and threats.

The industrial sector is undergoing rapid transformation through the use of data-driven automation capabilities and intelligent environments that possess the ability to analyze, decide, and act at the edge of chaos. Simultaneously, this evolution has enabled threats of intrusion and damage to national data assets, particularly violations of privacy resulting from the extensive points of contact due to the proliferation of diverse sensors capable of collecting vast amounts of data at any time and place.

From an environmental perspective, the increasing consumption of energy resources and its consequences in the production of greenhouse gases, due to the widespread trend of constant connectivity for all individuals through mobile phones, various wearables, and the development of fifth-generation wireless communication in the Internet of Things, has presented the world with challenges related to rare minerals and extensive disposal of hazardous waste on land and in the atmosphere. This situation necessitates the implementation of optimal management practices in the utilization of limited global resources.From a national security perspective, emerging cyber technologies can facilitate the effective entry of new actors such as multinational corporations, organized groups, and even individuals in the era of digital transformation. This

capability can profoundly impact global power dynamics, altering the conditions and rules of the playing field. It challenges traditional concepts of security, state-centric approaches to establishing security, and geographical dependencies of threats, leading to a transformation in the dimensions of vulnerability, methods of countering threats, and the multiplicity and granularity of actors, threat agents, and the tools and objectives of threats.

In this era, methods of espionage, deception, information infiltration, and assassination have been replaced by new cyber patterns. If the widespread and emerging consequences of these methods are overlooked, they will have strategic impacts on the national security of the country. Conversely, with coordinated national design and timely action, there is a significant opportunity to leverage this new capacity to strengthen the internal structure of national power through the creation of synergies among the pillars of governance.

Importance and Necessity

In discussing the importance of the topic, one can refer to the continuous epistemological position and the constant monitoring of rapid and significant developments in cyberspace due to its pervasive impact in countering strategic surprise. This foundation allows for the restructuring of organizational relationships among stakeholders and beneficiaries in the realm of the country's cyber governance, enabling national synergies to enhance efficiency and optimize resource consumption with an opportunity-oriented perspective. With this understanding, proactive actions against enemy objectives in the new security environment and coordinates can be achieved by transforming threats into opportunities arising from developments in cyberspace.

Undoubtedly, articulating the strategic importance of the impacts of emerging technologies draws the attention of the legislative domain of the country to the formulation of laws, protocols, and regulations, which inherently undergo a gradual process. Through this, the management of the space, provision of better services, promotion of production, and sustainable employment can be achieved in alignment with the realization of a resilient economy and other directives of the Supreme Leader (may his blessings be upon him).

In discussing the necessity of this research, one can refer to the instability and fragmentation in decision-making and action at the national level due to ambiguity, complexity, and uncertainty in understanding the macro impacts of emerging technologies across various dimensions of governance (in/with/on) cyberspace. The consequence of this is the emergence of strategic surprises against the evolving threats posed by adversaries in different aspects of national security, viewed through a comprehensive lens of security (in accordance with Copenhagen theory). The lack of integration and synergy in the realm of perception and action, coupled with managerial fragmentation among senior officials, leads to resource waste due to the instability of actions and hasty responses in managing diverse and emerging cyber phenomena at the national level, resulting in missed opportunities for proactive action.

For example, violations of privacy, deepfakes, dissemination of falsehoods in cyberspace, digital identity theft, and unauthorized access to national digital resources are among the modern examples of harm that require proactive behavior in the realm of criminalization. This includes timely updates to national laws and active participation in legislative bodies and international coalitions to address these issues.

Therefore, the main question of this research will be: "What impact do emerging cyber technologies have on national security?" This study aims to conduct an in-depth examination of emerging cyber technologies as an independent variable, initially identifying the inherent characteristics of these technologies. Subsequently, with a more abstract approach, the goal is to create a unique identity for the nature of emerging technologies as a unified entity with the capability for singular identification. Based on the specific characteristics obtained, the researcher seeks to identify the various impacts on different dimensions of national security.

With this approach, based on library studies and expert opinions, it is possible to prioritize the dimensions of national security affected by influential factors. In this context, the sub-questions are as follows: 1- "What are the specific characteristics of emerging cyber technologies?" 2- "What is the impact of each of the characteristics of emerging technologies on each dimension of national security?"

Therefore, the main objective is to identify the extent to which dimensions of national security are influenced by emerging cyber technologies. To this end, in the first step and as a secondary (intermediate) goal, the inherent characteristics related to the entirety of technologies will

be extracted as a unified concept. Subsequently, in the next step, the impact of these characteristics on each dimension of national security will be examined as the dependent variable of the research, from the perspective of expanded security. This approach aims to enhance the validity of the analysis results, distancing them from the continuous updates and changes in technology. For this purpose, a library study was conducted to explore the description, specifications, impacts, and consequences of each technology related to the four dimensions outlined in the selected definition of cyberspace for this research. Ultimately, their shared and overarching characteristics were extracted and categorized.

Therefore, the main objective is to identify the extent to which dimensions of national security are influenced by emerging cyber technologies. To achieve this, the first step, as an intermediate (secondary) goal, involves extracting the inherent characteristics related to the entirety of these technologies as a unified concept. Subsequently, in the next step, the impact of these characteristics on each dimension of national security will be examined as the dependent variable of the research, from the perspective of expanded security. This approach aims to enhance the validity of the analysis results, distancing them from the continuous updates and changes in technology. To this end, a library study was conducted to explore the description, specifications, impacts, and consequences of each technology related to the four dimensions outlined in the selected definition of cyberspace for this research. Ultimately, their shared and overarching characteristics were extracted and categorized.

Theoretical Foundations

Definition of Concepts

Cyberspace: Due to the differing perspectives and objectives emphasized by various governments and organizations over the years, multiple definitions of cyberspace have been presented with varying approaches to cybersecurity, and no comprehensive official definition has yet been agreed upon. A general overview of cyberspace definitions reveals four common perspectives: "network" as the core element of cyberspace, "data or information" along with its storage, analysis, access, transfer, exchange, and sharing, "human-machine interaction," and "time."

The most important idea derived from the prevalent definitions in the literature is that cyberspace is an artificial space related to physical, social, and intellectual domains, yet it exists as a self-regulating entity in a realm

independent of these domains (Hyunsung et al., 2018: 1844). Cyberspace is an informational space in which the global network creates an engaging world of communication and information resources. This information varies in location, classification, types, and forms (Kademi, Koltuksuz, 2020: 33).

The term "cyber" is derived from the word "cybernetics." In ancient Greece, cybernetics referred to the art of urban governance, the science of civil authority in society, and the art of ruling a nation, meaning "the science of control and processing of data in the domains of animals, machines, and society," which encompasses the results of all related sciences (Novikov, 2016: 2). With the convergence of the cyber-equipped world, the concept of cyberspace today must extend beyond physical, social, and intellectual spaces or Cyber-physical-social-thinking hyperspace(CPST) to include "informational space," as the space of "information" complements other cyber spaces and serves as energy for entities and a lifeline for the positioning and dynamics of cyberspace. Cyberspace is a "parallel world" arising from the intertwining of physical, social, informational, and intellectual spaces. It encompasses any information and entity that exists in the time and space of the digital world, with theoretical perspectives providing a space-time background for multiple cyber-formed spaces, including informational space (Kademi, Koltuksuz, 2021).

The U.S. Department of Defense defines the conventional and traditional understanding of cyberspace as a global domain and a part of the "information environment." "Cyberspace is a global domain, part of the information environment, consisting of interconnected networks of information technology infrastructures and the data residing therein, including the Internet, telecommunications networks, computer systems, processors, and embedded controllers. While cyberspace is a global domain within the information environment, it is one of five interconnected domains, which include other physical domains: air, land, maritime, and space." The information environment is also a collection of systems, individuals, and organizations that gather, process, publish, or take action on information. The information environment is divided into physical, cognitive, and informational dimensions (JP, 2013:6, 15).

As noted, the integration of various physical, social, and cognitive spaces with traditional cyberspace (as a purely informational space) has led to the emergence of a new concept known as "expanded cyberspace"

or public cyberspace. Expanded cyberspace fundamentally arises from the pervasive and ubiquitous communications between objects and the deep convergence of the aforementioned four spaces (Hyunseung et al., 2018: 1843).

In this research, the examination of emerging cyber technologies encompasses technologies from each of these four domains. As shown in Figure 1, this super cyberspace, with its pervasive connectivity and convergence of various spaces, has even influenced dimensions of philosophy, science, and cyber technology (Hyunseung, 2022: 3-5). Therefore, the operational definition of the desired cyberspace is "a space that results from the interpenetration, annexation, and unification of informational, physical, social, and cognitive spaces, characterized by the greatest inclusiveness based on pervasive and ubiquitous communications among its influential entities, and manifested as a unitary, complex, and time-dependent space through the mutual influence of human and non-human factors. Any element within this space that can collect, store, process, and exchange information and data online or offline is considered part of this space and will possess the capacity for influence." In this context, the research examined a wide range of technologies related to each of the four domains of cyberspace, focusing on their "nature, specific characteristics, consequences, and impacts" from the perspective of opportunities and threats at the national level.

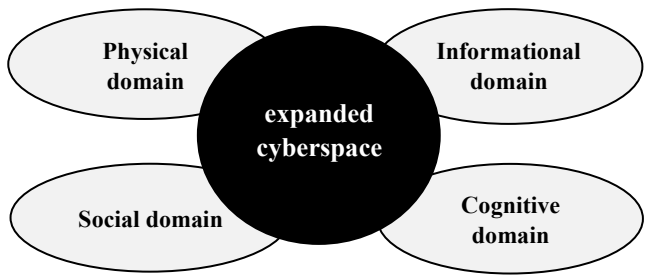


Figure 1: The selected model of the researcher for "expanded cyberspace" in this study represents the space resulting from the integration of four domains: informational, physical, social, and cognitive. This model is derived from the work of Kadami and Koltoxuoz (2021), as well as Hyunseung et al. (2018), and the University of Arizona model by Breen et al. (2020), all of which advocate for the integration of the aforementioned domains within the expanded cyberspace.

National Security: The concept of "self-preservation" or "protection of being" can be summarized into five categories: "protection of people's lives," "preservation of faith, beliefs, and values," "protection of territorial integrity," "maintenance of the economic and political system," and "preservation of the independence and sovereignty of the country." These five categories, by nature, constitute the essence of national security. The fundamental "philosophy of the existence of the state" is to safeguard security; however, it should not be expected that all governments regard specific and similar issues as their ordinary or vital interests within the framework of national security. The resources and interests of national security vary in nature and stability across different countries and times. For example, the definition of national interests for the government of Lebanon involves securing national security based on unity and territorial integrity, whereas for Japan, expanding markets and economic dominance globally are considered fundamental interests. This shift in security priorities, changes in values, or sacrificing them in favor of other values may sometimes occur out of necessity to prevent further harm to the national security framework. At other times, it happens voluntarily with the aim of adapting more effectively to changing internal and external conditions to facilitate the adoption of effective methods for stabilizing and strengthening the national security of each country (Hendiani, 1386: 14). Thus, the scope and boundaries of security remain inherently unclear due to its vastness (Bahush Fardaghi, 1396: 106). Given the complex nature of national security, particularly with the reciprocal impacts of cyberspace and emerging digital technologies, a new insight into understanding national security challenges has emerged as a dynamic phenomenon that disrupts established conditions, based on chaos theory grounded in critical thinking and learning (out-of-the-box thinking). In the contemporary world, where science and technology play significant roles in modeling complex solutions for a range of real-world security challenges, chaotic dynamics in theoretical modeling and real-life provide sustainable solutions for emerging challenges in demographics, politics, engineering, technology, and the enhancement of military technology capabilities.

Chaos theory can facilitate critical thinking and learning from the perspective of the interaction of chaos with politics, demography, sociology, economics, military decision-making processes, and other complex social phenomena in combating terrorism, political instability, informational insecurity, cybersecurity, and biometric security, the

outcome of which will be the development of national security (Ogechukwu et al., 2020: 1).

Attention to security requires consideration of elements of power; thus, if we count components of power instead of security components, we are not making an error. The components of power are divided into two categories. Soft components include leadership, morale, and external interaction (diplomacy), while hard components consist of military equipment and money. Regular assessment of the components of power and comparison with other governments, as well as understanding one's position in the hierarchy of global power, are essential steps in maintaining and stabilizing the security of society, as these concepts vary over time and across different geographical contexts. The components of security are highly interdependent, and therefore, they are mentioned without categorizing them into components of power (Moradi et al., 1399: 31-32).

Sources of power are generally in a state of flux. Over time, changes in the framework of thinking patterns(Shift paradigm) and mental models have shifted the source of power from military force to factors such as technology, education, and economy, aligned with the evolution of various national security doctrines. In each era, different sources of power have played a more significant role. Joseph Nye states that sources of power are never static and continue to experience change in today's world (Kohansal Kolkanari, Babaei, 1396: 10).

Given the constant changes in national power sources over time, it can be observed that in every period and condition of history, different resources have influenced national capabilities and power. Throughout history, the power of warfare, population, territorial extent, industry and rail networks, science and technology, nuclear weapons, and advanced technology-based economic power, as well as the current cyberspace, serve as sources of national power in all social, political, economic, and security domains (Pishgahi-Fard et al., 1393: 7).

The concept of smart power, which combines hard and soft power in the realm of national security, has led to the emergence of the notion of "smartening national security" in the present era. The outcome of this is the internal strengthening of national power and the transformation of threats into opportunities (Bayat, 1398: 377). In the domain of foreign policy, smart diplomacy arises from the foundation and context of this "smart power" (Izadi, 1393: 7). According to the teachings of Islam, strategies for "producing, maintaining, and reproducing national security"

include socialization, popularization, smartening, and promoting justice (previous source: 371).

From this perspective, all instances of cyberspace, including social networks and emerging capabilities of digital technologies, present a significant opportunity for strengthening the foundational aspects of national security of the Islamic Republic of Iran through cyber power components. The chosen definition of national security with a comprehensive approach intended for this research is "the ability of a nation to access resources and capabilities that enable it to safeguard against external and internal threats; repel foreign political, economic, cultural, and military domination; defend and protect its vital values in both peace and war; preserve the existence of the country and its territorial integrity; maintain a progressive increase in national power and capabilities across various domains; and successfully advance the balanced and dynamic development, reinforce national unity, and enhance the level of political participation in society" (same source: 36).

In this research, considering the expanding semantic scope and impact of the generalized cyberspace, the examination of its effect on national security is based on the Copenhagen security school. In the Copenhagen school, Barry Buzan, with a multifaceted approach to security, argues for the natural intertwining of various sectors (political, military, social, economic, and environmental) (Bakhshi Taliabi et al., 1396: 136). Therefore, the Copenhagen school offers a broader and clearer perspective on security compared to other security schools (Khani, 1399: 97), as it expands the concept of security and, by proposing five domains—military, political, economic, cultural/social, and environmental—effectively discards the unidimensional view of security from a purely military perspective. Nonetheless, it still considers the military domain as the most critical aspect of security (Bayat, 1398: 173). With a broad perspective derived from multiple contemporary security theories, the dimensions of national security encompass all aspects of human life from a governance standpoint[1] (Moradi et al., 1399: 33).

Technology: Technology is a harmonious and compatible combination of hardware, software, and firmware that finds its true meaning and significance within the framework of an infrastructural network. Technology is not merely a tool or knowledge for performing a task or an

[1] Political, security, military/defensive, informational, economic, cultural, social, legal (judicial), environmental, food, psychological/moral, and outer space.

idea and design; rather, it possesses a nature akin to society, encompassing all related social interactions, and can only be understood, managed, and led with such a perspective. The main components of technology, which are interrelated and complementary, include hardware, software, firmware, and support networks (Mahmoudzadeh, 1389: 64).

Technology: Technology is a harmonious and compatible combination of hardware, software, and firmware that finds its true meaning and significance within the context of an infrastructural network. Technology is not merely a tool or knowledge for performing a task or an idea and design; rather, it possesses a nature similar to society, encompassing all related social interactions, and can only be understood, managed, and led with such a perspective. The main components of technology, which are interrelated and complementary, include hardware, software, firmware, and support networks (Mahmoudzadeh, 1389: 64).

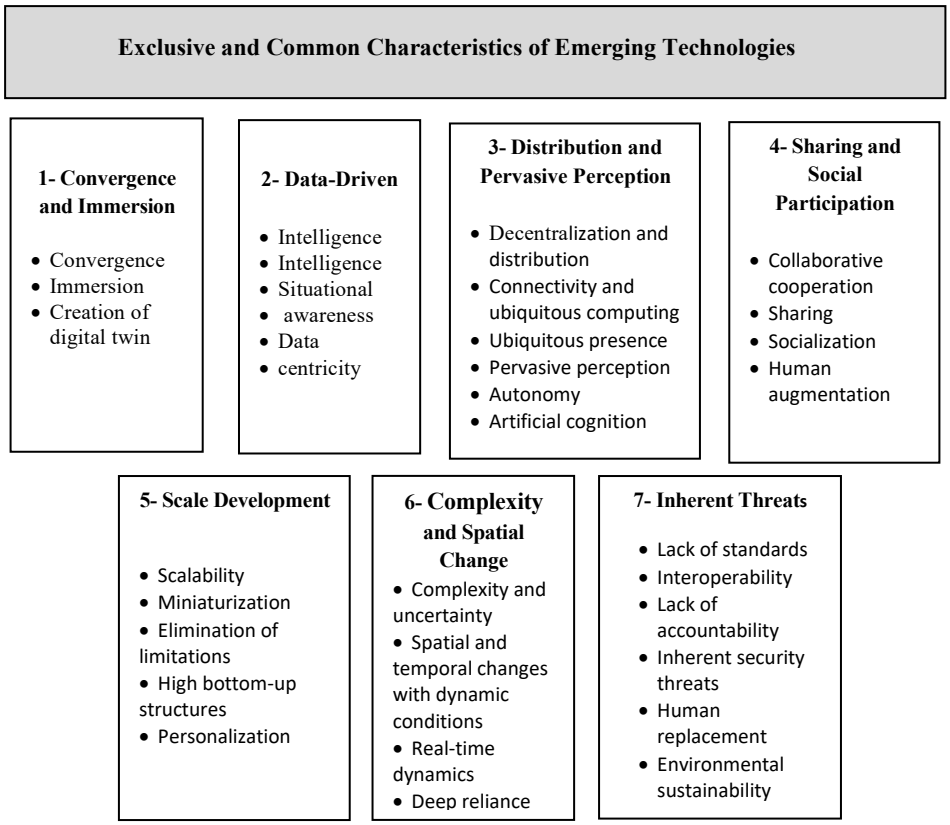
Emerging technology: In the next 10 to 15 years, it will lead to significant changes in society, social institutions, and the economy. Emerging technology possesses a fundamentally novel nature, characterized by rapid growth and, of course, ambiguity and uncertainty regarding its outcomes (Rotolo et al., 2016: 34). Emerging technology is one that shows high potential but has not yet demonstrated its value or reached any form of collective agreement (Cozzens et al., 2010: 364), and its forms, capabilities, limitations, and precise applications remain unclear (Stahl, 2011: 3-4). The general characteristics of emerging technologies (IT) include "uncertainty, network effects[1], high costs, social and ethical concerns, limitations for specific countries, and a lack of research and studies" (Halaweh, 2013: 108).

Specific characteristics of emerging cyber technologies: To achieve the research objective (examining the impact of emerging cyberspace technologies on national security), the use of specific and common characteristics of these technologies serves as the operational criterion. Given that these characteristics are at a higher level of abstraction and conceptualization than the emerging technologies themselves, which are constantly changing and being updated, they allow for the examination of impact in a more stable mental environment due to fewer changes in the surrounding conditions of the analytical environment. Therefore, the

[1].According to the law of network effects, the power and value of a network increase with the number of individuals who use or are connected to that network (Metcalfe, 1995).

lifespan and credibility of the obtained results will be enhanced, leading to greater reliability.

Figure 2: General classification of the characteristics of emerging technologies, in seven main categories (research findings of the author)



For this purpose, through a detailed examination of articles, books, and relevant scientific sources, the "description, characteristics, and consequences of emerging technologies" were studied. Subsequently, by scrutinizing the details of each technology, a holistic approach was adopted to infer the distinctive attributes of emerging technologies. Considering the researcher's selected model of cyberspace—due to the comprehensive inclusiveness of the generalized cyberspace—in order to identify the impact of cyber technologies across all physical, informational, social, and cognitive domains on national security, with particular attention to the occurrence of convergence, synergy, and the integration and unification of technological domains, the identified characteristics were derived (Figure 2).

In general, emerging cyber technologies possess a shared nature, meaning that all these characteristics relatively apply to each of the technologies. By examining the obtained results, and with consideration of semantic and functional similarities of the characteristics within each category, the specific and common attributes describing the nature of emerging technologies were classified into seven main categories (Figure 2).

The first characteristic, "Convergence and Immersion," refers to the attributes of technological integration and the fusion of physical and virtual spaces, as well as the development of digital twins (digital counterparts of any entity) in facilitating the immersion of both human and non-human entities within an interactive and intelligent environment (Dotsenko, 2017; Roco, 2020; Dwivedi et al., 2022; Yong-Woon et al., 2021).

The second characteristic, "Data-Driven Intelligence," addresses the attribute of cognitive situational awareness derived from data analysis (Priyadarshini & Cotton, 2020; Andrade & Yoo, 2019; Thiner et al., 2017).

The third characteristic, "Distribution and Pervasive Perception," refers to the attribute of decentralization and distribution in autonomous decision-making, which stems from the features of connectivity and ubiquitous computing, pervasive perception (in edge computing), and the advancement of artificial cognition in intelligent agents such as robots (Breno & Luiz, 2020; Scott, 2018; Cadell, 2020; Fei et al., 2021).

The fourth characteristic, "Sharing and Social Participation," concerns the development of collaborative cooperation and the social behavior of intelligent agents based on data sharing. This shared approach contributes to the enhancement of life and the augmentation of humans and society, while simultaneously generating unprecedented threats to humanity (Bussu et al., 2022; Schwab, 2016; Atlam et al., 2018).

The fifth characteristic, "Scale Development," refers to the elimination of limitations, miniaturization, and scalability of influencing factors, the outcome of which is the expansion of bottom-up structures affecting governance and the personalization of services in accordance with needs (Cheraghi, 2021; Lee & Moon, 2020; Schmidt, 2016; Fernando, 2019; Trevor et al., 2018).

The sixth characteristic, "Complexity and Spatial Change," arises from the growing uncertainty and the paradigm shifts in concepts resulting from profound dependence on technology and real-time dynamics (Reding et al., 2023; Montasari et al., 2020; European Union, 2019; Chisnall, 2020).

Ultimately, the seventh characteristic is "inherent threats," which arise due to properties such as accountability issues, lack of standards, increasing inequalities, the gradual replacement of humans, the erosion of human dignity, challenges to transparency, environmental concerns, and environmental resilience. This is further emphasized by the inherent nature of threats resulting from the unprecedented expansion of contact points and the augmentations caused by the intelligence of autonomous elements and the exponential growth of self-decisive factors. On the other hand, the inherently ambiguous nature resulting from the phenomenon of divergence following the integration and convergence of technologies is considered a cause of these threats (Rocco, 2020; Ryan, 2020; Zachary, 2016; Attiah and Farah, 2014; Meijer et al., 2019; Tidjon and Khomh, 2022).

The operational definitions of each of the extracted characteristics are presented in Table1.

Table 1: Definition of characteristics of emerging cyber technologies, derived from the results of a thorough review of scientific sources.

Main category of technology characteristic	Operational definition (derived from the overall concepts obtained from research sources)
Convergence and immersion	"The integration and blending of emerging sciences and technologies has led to uncertainty and ambiguity in the predictability of the outcomes, products, and impacts of this convergence. The resulting convergence has expanded the meaning of immersion due to the seamless and boundless amalgamation of physical and virtual spaces. This is facilitated by the prevalence of multimedia and the concept of 'true virtuality' (engaging all human senses instead of just some in a virtual reality), creating an 'always-on' environment where the perpetual activity of the digital twin of every human and non-human entity in an interactive and intelligent environment enables the realization of digital eternity."
Data-driven intelligence	"The development of systems with varying degrees of autonomy that possess capabilities for perception, learning, abstraction, reasoning, decision-making, and autonomous action to achieve specific goals is characterized by their cognitive situational awareness, enabling them to predict future events. All these enhancements stem from the datafication of all aspects of human life, creating new values that position data as a national digital asset, confronting the challenge of spatial unity and the evasion of national borders."
Distributedness and pervasive perception	"The nature of distributedness and lack of central control, due to the constant connectivity between individuals, objects, and pervasive computing, enables computational devices to adapt their behavior by assessing the physical context (including people, objects, events, and

Main category of technology characteristic	Operational definition (derived from the overall concepts obtained from research sources)
	conditions). Additionally, the distributed intelligence of elements necessitates the ability to influence the environment with cyber autonomy grounded in situational awareness. Consequently, this develops the concept of a cyber brain capable of artificial thinking, enhancing its self-learning capabilities from the perceived surrounding environment."
Social sharing and participation	The collaborative behavior of cyber-physical systems, based on social situational awareness and distributed network intelligence, along with collective intelligence, enables the integration of systems and robots in a social context. In interaction with society, this is grounded in AI that is socially aware and combines social characteristics. This enhanced intelligence is referred to as 'artificial social intelligence.' Participation based on data sharing occurs within the framework of agreements and legal protocols. Additionally, sharing assets in the form of ownership and collaborative consumption is achievable in a participatory and circular economy. Overall, this social participation between humans and machines, as well as among humans, in an intelligent environment can lead to human augmentation and, if socially integrated, result in social enhancement."
Scale development	"To overcome the increasing complexity and expertise resulting from the rapid integration of emerging technologies, the ability to adapt performance and cost in response to environmental changes is an operational necessity for the competitiveness and resilience of any organization. The removal of physical limitations due to the development of emerging technologies has played a significant role in accessibility, ease of access, and the reduction of user costs for the public. This has resulted in the development of open governance with a bottom-up supervisory structure, enabling the provision of mass personalized services. However, this personalization can also be accompanied by numerous threats at the national level."
Complexity and spatial change	"With the multitude of interacting elements that have networked connections in a self-organizing, universal, and open intelligent environment, the growth of nested complexity without the presence of defined causal relationships is a certainty. The result will be a transformation in mental paradigms and traditional rules of the game. Additionally, the development of high-performance computing at the edge, with deep reliance on technology in cyber-physical-cognitive-social systems, expands the capability for dynamic interaction and real-time self-decision-making, fundamentally altering the nature of the future world."
Threat generation	"Due to uncertainty, ambiguity, complexity, and rapid and profound changes resulting from technological developments, as well as the emergence of unknowns following the divergence phase after convergence in the technology development cycle, no specific standards have been established for emerging issues. Additionally, ethical challenges in many

Main category of technology characteristic	Operational definition (derived from the overall concepts obtained from research sources)
	areas pose significant obstacles. Privacy issues, ownership, auditing, accountability, liability, compensation for damages, lack of legal evidence and definitive criminalization in judgments, the possibility of 3D printing weapons, growing inequality, discrimination, social fragmentation, the development of class gaps, the emergence of new power polarizations in the geometry of the new global order, violations of human dignity, challenges of transparency, digital human rights, cross-border data challenges, lack of or biased global laws (in the legislative war), increased levels of contact, cultural displacement, ambiguity in measuring the circular economy, information laundering challenges, human replacement (transformation in self-identity), proposals for robot rights, and environmental resilience are unresolved issues and challenges in this domain. The general inference of this situation aligns with the concept of widespread threat generation."

Research Methodology

Considering the examination of the impact of emerging cyber technologies on national security in this research, a mixed-methods approach (qualitative-quantitative) has been identified as the most suitable method. This approach utilizes both qualitative and quantitative analyses; the qualitative analysis is based on the opinions and perspectives of informed experts, while the quantitative findings from the qualitative section are validated through a researcher-constructed questionnaire utilizing the insights of elites and specialists in the field.

Ultimately, the impact of emerging cyber technologies on national security is elucidated, providing actionable insights for policymakers and governance managers. To conduct this research, after reviewing the theoretical foundations, comparative studies, and gathering opinions from experts in the field of information technology, the inherent characteristics of emerging technologies were identified and categorized. This categorization was evaluated through a semi-open questionnaire administered to the experts. In the next phase, the impact of the abstract characteristics of technology on dimensions of national security was assessed using a closed questionnaire and quantitative methods. The dimensions of national security, based on the Copenhagen School and a broadened security perspective, were considered across four areas: military/defense, political/security, economic, and cultural/social. The provisions related to the environmental dimension were analyzed in a reduced capacity and were integrated into the aforementioned dimensions due to their relatively limited content compared to other topics.

Statistical Population, Sample Size, and Sampling Method

The statistical population for the qualitative aspect includes both important and accessible documents and "social informants" (experts and elites in the field of cyberspace) that will be examined and analyzed. In the quantitative section, the statistical population also consists of these social informants. Social informants include:

Officials, executive managers, and experts in the field of cyberspace and emerging technologies with a minimum of 15 years of specialized experience.

Elites, scholars, and thinkers in the field of cybersecurity across social, cultural, political, defense, security, executive, and technological dimensions, possessing advanced academic degrees in this area.

Sampling Method

The sampling method was conducted in two sections, qualitative and quantitative, and involved two types. In the area of documents, all accessible documents were collected and utilized using a purposive sampling method. In the section concerning social and cybersecurity informants, a selective sampling method was employed to determine the required sample based on the theoretical saturation principle. Accordingly, using Morgan's table based on Cochran's formula, a sample size of 44 was calculated for a margin of error of 0.05, while in practice, 47 individuals participated.

Method and Tools for Data Collection

The library method and questionnaires in the form of field operations were used as the data collection methods. The data collection tools included a researcher-constructed questionnaire and document analysis. For data analysis, both descriptive and inferential statistics were employed using SPSS version 23. The validity of the questionnaire was calculated based on the "content validity" method and the Lawshe table, yielding a value of 0.6, which is acceptable. Additionally, the average Cronbach's alpha of 0.723 for the questionnaires indicates their reliability.

Data analysis was conducted in two parts: descriptive and inferential. In the descriptive section, descriptive statistics (frequency tables and charts, mean, standard deviation, etc.) were utilized. In the inferential section, the "Kolmogorov-Smirnov" test was employed to assess normality, the "Chi-square" test was used for ranking the data, and multiple linear regression, analysis of variance (ANOVA), and the F-test

were applied to ascertain the correlation between variables and the impact of independent variables on the dependent variable.

Analysis of Findings

Ranking of the Characteristics of Emerging Cyber Technologies: To rank the characteristics of emerging cyber technologies, a questionnaire was distributed, and data was collected from experts using a seven-point Likert scale for evaluating the characteristics. According to the table below, the obtained average scores are presented:

Table No. (2): Ranking of the Characteristics of Emerging Cyber Technologies

Characteristics	Average Score	Rank
Data-driven Intelligence	6.4	First
Complexity and Fluidity of Space	6.3	Second
Threat Generation	6.2	Third
Convergence and Immersion	6.1	Fourth
Distribution and Widespread Perception	5.9	Fifth
Sharing and Social Participation	5.8	Sixth
Scale Development	5.6	Seventh

Ranking of National Security Dimensions

Based on the average scores obtained, data-driven intelligence is identified as the most important dimension of emerging cyber technologies, with an average score of 4.6 out of 7. Complexity and changing environments rank second with an average score of 3.6, followed by threat generation in third place with an average score of 2.6, and finally, the development of scales, which ranks last with an average score of 6.5.

To rank the dimensions of national security, a questionnaire was distributed, and information was collected from experts using a seven-point Likert scale for evaluating the dimensions. The average scores obtained are presented in the table below:

Table 3: Ranking of National Security Dimensions

Dimensions	Average Scores	Ranking
Political Security	Political Security: 6.7	First:
Military Defense	Military Defense: 6.2	Second:
Cultural Social	Cultural Social: 5.8	Third:
Economic	Economic: 5.3	Fourth:

Analysis of Average Scores

Based on the average scores obtained, the political-security dimension is identified as the most important aspect of national security, with an average score of 6.7 out of 7. The military-defense dimension ranks second with an average score of 6.2, followed by the cultural-social dimension in third place with an average score of 5.8, and lastly, the economic dimension, which ranks fourth with an average score of 5.3. It is important to note that, from the experts' perspective, all dimensions hold significant value and received scores above the average.Analysis of the Impact of Emerging Cyber Technology Characteristics on National Security

Impact of "Convergence and Immersion" of Emerging Cyber Technologies on National Security:

Table 4: Summary of the Regression Model

Model Summary b				
Model	**Correlation Coefficient (R)**	**Coefficient of Determination (R^2)**	**Adjusted Correlation Coefficient (R)**	**Standard Error of Estimate**
1	0.411a	0.168	0.171	3.4785
a. Dependent Variable : National Security				
b. Predictors (Constant): Convergence and Immersion				

The table above shows the model summary. The value of the correlation coefficient (R) between the variables is 0.411, indicating a moderate and direct correlation between the independent variable (convergence and immersion of emerging cyber technologies) and the dependent variable of the study. However, the adjusted coefficient (R^2) is 0.171, which indicates that 17.1% of the total national security is dependent on the independent variable of the study (convergence and immersion of emerging cyber technologies). Therefore, the impact of the independent variable on the dependent variable is 17.1%, and it can be stated that convergence and immersion of emerging cyber technologies influence national security.

Investigating the Impact of Convergence and Immersion of Emerging Cyber Technologies on Dimensions of National Security.To examine the impact of emerging cyber technologies on dimensions of national security, a linear multiple regression analysis has been conducted. For the ease of presenting the results of the statistical tests performed, the summary of the findings is provided in Table 5.

Table 5: Summary of Relationships Between Variables

Row	Independent Variable	Dimensions of the Dependent Variable	Correlation Coefficient (R)	Coefficient of Determination (R^2)	F-Test	Significance Level
1	Convergence and Immersion	Political Security	0.413	0.170	12.207	0.001
2		Military Defense	0.489	0.239	36.209	0.000
3		Cultural Social	0.459	0.210	9.954	0.000
4		Economic	0.364	0.132	1.124	0.012

Based on the results, it can be stated that the convergence and immersion of emerging cyber technologies have the highest direct and positive relationship with the military-defensive dimension of national security, with a correlation coefficient of 0.489. According to the provided coefficient of determination, the convergence and immersion of emerging cyber technologies explain and influence 23.9% of the military-defensive dimension of national security. In the second rank, the convergence and immersion of emerging cyber technologies show a direct and positive relationship with the cultural-social dimension of national security, with a correlation coefficient of 0.459. Based on the provided coefficient of determination, the convergence and immersion of emerging cyber technologies explain and influence 21% of the cultural-social dimension of national security. In the third rank, the convergence and immersion of emerging cyber technologies have a direct and positive relationship with the political-security dimension of national security, with a correlation coefficient of 0.413. According to the provided coefficient of determination, the convergence and immersion of emerging cyber technologies explain and influence 17% of the political-security dimension of national security. In the fourth rank, the convergence and immersion of emerging cyber technologies show a direct and positive relationship with the economic dimension of national security, with a correlation coefficient of 0.364. Based on the provided coefficient of determination, the convergence and immersion of emerging cyber technologies explain and influence 13.2% of the economic dimension of national security.

The Impact of Data-Driven Intelligence of Emerging Technologies on National Security

The table 6 summarizes the model. The correlation coefficient (R) between the variables is 0.563, indicating a strong and direct correlation between the independent variable (data-driven intelligence of emerging cyber technologies) and the dependent variable of the study:

Table No. (6): Summary of the Regression Model

Model Summary b				
Model	**Correlation Coefficient (R)**	**Coefficient of Determination (R^2)**	**Adjusted Correlation Coefficient (R)**	**Standard Error of Estimate**
1	0.563a	0.316	0.319	3.8963
a. Dependent Variable : National Security				
b. Predictors: (Constant): Data-Driven Intelligence				

However, the adjusted R^2 value of 0.319 shows that 31.9% of the overall national security is dependent on the independent variable of the study (data-driven intelligence of emerging cyber technologies). Therefore, the impact of the independent variable on the dependent variable is 31.9%, suggesting that data-driven intelligence of emerging cyber technologies influences national security.

Examining the Impact of Data-Driven Intelligence of Emerging Cyber Technologies on Dimensions of National Security

To examine the impact of data-driven intelligence of emerging cyber technologies on dimensions of national security, a multiple linear regression was conducted. For the sake of clarity in presenting the results of the statistical tests performed, a summary of the research findings is provided in Table 7.

Table No. (7): Summary of Relationships Between Variables

Row	Independent Variable	Dimensions of the Dependent Variable	Correlation Coefficient (R)	Coefficient of Determination (R^2)	F-Test	Significance Level
1	Data-Driven Intelligence	Political Security	0.509	0.259	17.213	0/000
2		Military Defense	0.587	0.344	698.213	0/000
3		Cultural Social	0.523	0.273	667.212	0/000
4		Economic	0.501	0.251	557.211	0/000

Based on the results, it can be stated that data-driven intelligence of emerging cyber technologies has the highest direct and positive correlation of 0.587 with the military-defense dimension of national security. According to the provided coefficient of determination, data-driven intelligence of emerging cyber technologies accounts for 34.4% of the military-defense dimension of national security and influences it. In

second place, data-driven intelligence of emerging cyber technologies has a direct and positive correlation of 0.523 with the socio-cultural dimension of national security. Based on the provided coefficient of determination, data-driven intelligence of emerging cyber technologies accounts for 27.3% of the socio-cultural dimension of national security and influences it. In third place, data-driven intelligence of emerging cyber technologies has a direct and positive correlation of 0.509 with the political-security dimension of national security. According to the provided coefficient of determination, data-driven intelligence of emerging cyber technologies accounts for 25.9% of the political-security dimension of national security and influences it. In fourth place, data-driven intelligence of emerging cyber technologies has a direct and positive correlation of 0.501 with the economic dimension of national security. According to the provided coefficient of determination, data-driven intelligence of emerging cyber technologies accounts for 25.1% of the economic dimension of national security and influences it.

The Impact of "Social Sharing and Participation" of Emerging Technologies on National Security

Table No. (8): Summary of the Regression Model

Model Summary b				
Model	**Correlation Coefficient (R)**	**Coefficient of Determination (R^2)**	**Adjusted Correlation Coefficient (R)**	**Standard Error of Estimate**
1	0.366a	0.133	0.137	3.0321
a. Dependent Variable : National Security				
b. Predictors (Constant): social sharing and participation of emerging cyber technologies				

The table above summarizes the model. The correlation coefficient (R) between the variables is 0.366, indicating a moderate (negative) and direct correlation between the independent variable (social sharing and participation of emerging cyber technologies) and the dependent variable of the research. However, the adjusted coefficient of determination (R^2), which is 0.137, indicates that 13.7% of the overall national security is dependent on the independent variable of the research (social sharing and participation of emerging cyber technologies). Therefore, the impact of the independent variable on the dependent variable is 13.7%, suggesting that social sharing and participation of emerging cyber technologies influence national security.

Examining the Impact of Social Sharing and Participation of Emerging Cyber Technologies on Dimensions of National Security.To examine the impact of social sharing and participation of emerging cyber technologies on dimensions of national security, a multiple linear regression analysis was conducted. For the convenience of presenting the results of the statistical tests performed, the summary of the research findings is outlined in Table 9:

Table No. (9)

Row	Independent Variable	Dimensions of the Dependent Variable	Correlation Coefficient (R)	Coefficient of Determination (R^2)	F-Test	Significance Level
1	Social Sharing and Participation	Political Security	0.395	0.156	209.214	80/00
2		Military Defense	0.362	0.131	209.411	90/00
3		Cultural Social	0.321	0.103	208.563	.30/
4		Economic	0.311	0.096	209.324	.40/

According to the presented results, it can be stated that social sharing and participation of emerging cyber technologies have the highest direct and positive correlation of 0.395 with the political-security dimension of national security. Based on the provided coefficient of determination, social sharing and participation of emerging cyber technologies explain 15.6% of the political-security dimension of national security and influence it. In second place, social sharing and participation of emerging cyber technologies have a direct and positive correlation of 0.362 with the military-defense dimension of national security. According to the provided coefficient of determination, social sharing and participation of emerging cyber technologies explain 13.1% of the military-defense dimension of national security and influence it. In third place, social sharing and participation of emerging cyber technologies have a direct and positive correlation of 0.321 with the socio-cultural dimension of national security. Based on the coefficient of determination, social sharing and participation of emerging cyber technologies explain 10.3% of the socio-cultural dimension of national security and influence it. In fourth place, social sharing and participation of emerging cyber technologies have a direct and positive correlation of 0.311 with the economic dimension of national security. According to the provided coefficient of determination, social sharing and participation of emerging

cyber technologies explain 9.6% of the economic dimension of national security and influence it.

The Impact of "Threat Creation" of Emerging Technologies on National Security

Table No. (10): Summary of the Regression Model

Model Summary B				
Model	**Correlation Coefficient (R)**	**Coefficient of Determination (R^2)**	**Adjusted Correlation Coefficient (R)**	**Standard Error of Estimate**
1	0.303 a	0.091	0.093	3.1254
a. Dependent Variable : National Security				
b. Predictors (Constant): Threat Creation				

The table above summarizes the model. The correlation coefficient (R) between the variables is 0.303, indicating a moderate (negative) correlation between the independent variable (threat creation of emerging cyber technologies) and the dependent variable of the research. However, the adjusted coefficient of determination (R^2), which is 0.093, shows that 9.3% of the overall national security is dependent on the independent variable of the research (threat creation of emerging cyber technologies). Therefore, the impact of the independent variable on the dependent variable is 9.3%, suggesting that threat creation of emerging cyber technologies influences national security.

Examining the Impact of Threat Creation by Emerging Cyber Technologies on Dimensions of National Security

To investigate the effect of threat creation by emerging cyber technologies on dimensions of national security, a multiple linear regression analysis was conducted. For the convenience of presenting the results of the statistical tests performed, the summary of the research findings is outlined in the table below:

Examining the Impact of Threat Creation by Emerging Cyber Technologies on Dimensions of National Security

To investigate the effect of threat creation by emerging cyber technologies on dimensions of national security, a multiple linear regression analysis was

conducted. For the convenience of presenting the results of the statistical tests performed, the summary of the research findings is outlined in Table 11:

Table No. (11): Summary of Relationships Between Variables

Row	Independent Variable	Dimensions of the Dependent Variable	Correlation Coefficient (R)	Coefficient of Determination (R^2)	F-Test	Significance Level
1	Threat Creation	Political Security	0.314	0.098	208.142	0090/
2		Military Defense	0.306	0.093	208.336	012 0/
3		Cultural Social	0.289	0.083	207.119	0320/
4		Economic	0.283	0.080	207.003	0440/

According to the presented results, it can be stated that threat creation by emerging cyber technologies has the highest direct and positive correlation of 0.314 with the political-security dimension of national security. Based on the provided coefficient of determination, threat creation by emerging cyber technologies explains 9.8% of the political-security dimension of national security and influences it. In second place, threat creation by emerging cyber technologies has a direct and positive correlation of 0.306 with the military-defense dimension of national security. According to the provided coefficient of determination, threat creation by emerging cyber technologies explains 9.3% of the military-defense dimension of national security and influences it. In third place, threat creation by emerging cyber technologies has a direct and positive correlation of 0.289 with the socio-cultural dimension of national security. Based on the provided coefficient of determination, threat creation by emerging cyber technologies explains 8.3% of the socio-cultural dimension of national security and influences it. In fourth place, threat creation by emerging cyber technologies has a direct and positive correlation of 0.283 with the economic dimension of national security. According to the provided coefficient of determination, threat creation by emerging cyber technologies explains 8% of the economic dimension of national security and influences it.

The Impact of "Complexity and Changing Landscape" of Emerging Technologies on National Security.

Table No. (12): Summary of the Regression Model

Model Summary b				
Model	**Correlation Coefficient (R)**	**Coefficient of Determination (R^2)**	**Adjusted Correlation Coefficient (R)**	**Standard Error of Estimate**
1	0.414 a	0.171	0.173	3.3214
a. Dependent Variable : National Security				
b. Predictors (Constant): complexity and changing landscape				

The table above summarizes the model. The correlation coefficient (R) between the variables is 0.414, indicating a relatively strong and direct correlation between the independent variable (complexity and changing landscape of emerging cyber technologies) and the dependent variable of the research. However, the adjusted coefficient of determination (R^2), which is 0.173, shows that 17.3% of the overall national security is dependent on the independent variable of the research (complexity and changing landscape of emerging cyber technologies). Therefore, the impact of the independent variable on the dependent variable is 17.3%, suggesting that complexity and changing landscape of emerging cyber technologies influences national security.

Examining the Impact of Complexity and Changing Landscape of Emerging Cyber Technologies on Dimensions of National Security

To investigate the impact of complexity and changing landscape of emerging cyber technologies on dimensions of national security, a multiple linear regression analysis was conducted. Due to the reduction in the presentation of statistical tables, the summary of the impact is provided in the table below. For the convenience of presenting the results of the statistical tests performed, the summary of the research findings is outlined in Table 13:

Table No. (13): Summary of Relationships Between Variables

Row	Independent Variable	Dimensions of the Dependent Variable	Correlation Coefficient (R)	Coefficient of Determination (R^2)	F-Test	Significance Level
1	complexity and changing landscape	Political Security	0.419	0.175	210.17	0000/
2		Military Defense	0.425	0.180	211.554	0000/
3		Cultural Social	0.401	0.160	210.665	0000/
4		Economic	0.404	0.163	209.362	0000/

According to the presented results, it can be stated that complexity and changing landscape of emerging cyber technologies have the highest direct and positive correlation of 0.425 with the military-defense dimension of national security. Based on the provided coefficient of determination, complexity and changing landscape of emerging cyber technologies explain 18% of the military-defense dimension of national security and influence it. In second place, complexity and changing landscape of emerging cyber technologies have a direct and positive correlation of 0.419 with the political-security dimension of national security. According to the provided coefficient of determination, complexity and changing landscape of emerging cyber technologies explain 17.5% of the political-security dimension of national security and influence it. In third place, complexity and changing landscape of emerging cyber technologies have a direct and positive correlation of 0.404 with the economic dimension of national security. Based on the provided coefficient of determination, complexity and changing landscape of emerging cyber technologies explain 16.3% of the economic dimension of national security and influence it. In fourth place, complexity and changing landscape of emerging cyber technologies have a direct and positive correlation of 0.401 with the socio-cultural dimension of national security. According to the provided coefficient of determination, complexity and changing landscape of emerging cyber technologies explain 16% of the socio-cultural dimension of national security and influence it.

The Impact of "Scale Development" of Emerging Technologies on National Security

Table No. (14): Summary of the Regression Model

Model Summary b				
Model	**Correlation Coefficient (R)**	**Coefficient of Determination (R^2)**	**Adjusted Correlation Coefficient (R)**	**Standard Error of Estimate**
1	0.3444 a	0.118	0.121	3.003

The table above summarizes the model. The correlation coefficient (R) between the variables is 0.344, indicating a moderate (downward) correlation between the independent variable (scale development of emerging cyber technologies) and the dependent variable of the research. However, the adjusted coefficient of determination (R^2), which is 0.121, shows that 12.1% of the overall national security is dependent on the independent variable of the research (scale development of emerging cyber technologies). Therefore, the impact of the independent variable on the dependent variable is 12.1%, suggesting that scale development of emerging cyber technologies influences national security.

Table No. (15): Summary of Relationships Between Variables

Row	**Independent Variable**	**Dimensions of the Dependent Variable**	**Correlation Coefficient (R)**	**Coefficient of Determination (R^2)**	**F-Test**	**Significance Level**
1	complexity and changing landscape	Political Security	0.453	0.206	210.141	0010/
2		Military Defense	0.468	0.219	211.236	0000/
3		Cultural Social	0.442	0.195	210.333	0050/
4		Economic	0.431	0.185	209.217	0090/

Based on the results, it can be stated that scale development of emerging cyber technologies has the highest direct and positive correlation of 0.468 with the military-defense dimension of national security. According to the provided coefficient of determination, scale development of emerging cyber technologies explains 21.9% of the military-defense dimension of national security and influences it. In second place, scale development of emerging cyber technologies has a direct and positive correlation of 0.453 with the political-security dimension of national security. Based on the provided coefficient of determination, scale development of emerging cyber technologies explains 20.6% of the political-security dimension of

national security and influences it. In third place, scale development of emerging cyber technologies has a direct and positive correlation of 0.442 with the socio-cultural dimension of national security. According to the provided coefficient of determination, scale development of emerging cyber technologies explains 19.5% of the socio-cultural dimension of national security and influences it. In fourth place, scale development of emerging cyber technologies has a direct and positive correlation of 0.431 with the economic dimension of national security. Based on the provided coefficient of determination, scale development of emerging cyber technologies explains 18.5% of the economic dimension of national security and influences it.

The Impact of "Distributedness and Ubiquitous Perception" of Emerging Technologies on National Security

Table No. (16): Summary of the Regression Model

Model Summary b				
Model	**Correlation Coefficient (R)**	**Coefficient of Determination (R^2)**	**Adjusted Correlation Coefficient (R)**	**Standard Error of Estimate**
1	0.369 a	0.136	0.139	3.2247
a. Dependent Variable : National Security				
b. Predictors (Constant): distributedness and ubiquitous perception				

The table above summarizes the model. The correlation coefficient (R) between the variables is 0.369, indicating a moderate (downward) correlation between the independent variable (distributedness and ubiquitous perception of emerging cyber technologies) and the dependent variable of the research. However, the adjusted coefficient of determination (R^2), which is 0.139, shows that 13.9% of the overall national security is dependent on the independent variable of the research (distributedness and ubiquitous perception of emerging cyber technologies). Therefore, the impact of the independent variable on the dependent variable is 13.9%, suggesting that distributedness and ubiquitous perception of emerging cyber technologies influences national security.

Examining the Impact of Distributedness and Ubiquitous Perception of Emerging Cyber Technologies on Dimensions of National Security

To investigate the impact of distributedness and ubiquitous perception of emerging cyber technologies on dimensions of national security, a multiple

linear regression analysis was conducted. For the convenience of presenting the results of the statistical tests performed, the summary of the research findings is outlined in Table 17:

Table No. (17): Summary of Relationships Between Variables

Row	Independent Variable	Dimensions of the Dependent Variable	Correlation Coefficient (R)	Coefficient of Determination (R^2)	F-Test	Significance Level
1	Distributedness and Ubiquitous Perception	Political Security	0.391	0.152	209.114	0010/
2		Military Defense	0.377	0.142	209.856	0020/
3		Cultural Social	0.362	0.131	208.887	0050/
4		Economic	0.359	0.128	208.665	0090/

Based on the results presented, it can be stated that distributedness and ubiquitous perception of emerging cyber technologies have the highest direct and positive correlation of 0.391 with the political-security dimension of national security. According to the provided coefficient of determination, distributedness and ubiquitous perception of emerging cyber technologies explain 15.2% of the military-defense dimension of national security and influence it.

In second place, distributedness and ubiquitous perception of emerging cyber technologies have a direct and positive correlation of 0.377 with the military-defense dimension of national security. According to the provided coefficient of determination, distributedness and ubiquitous perception of emerging cyber technologies explain 14.2% of the military-defense dimension of national security and influence it. In third place, distributedness and ubiquitous perception of emerging cyber technologies have a direct and positive correlation of 0.362 with the socio-cultural dimension of national security. According to the provided coefficient of determination, distributedness and ubiquitous perception of emerging cyber technologies explain 13.1% of the socio-cultural dimension of national security and influence it. In fourth place, distributedness and ubiquitous perception of emerging cyber technologies have a direct and positive correlation of 0.359 with the economic dimension of national security. According to the provided coefficient of determination, distributedness and ubiquitous perception of emerging cyber technologies

explain 12.8% of the economic dimension of national security and influence it.

Conclusion and Recommendations

It can be stated that the rapid and profound transformations of cyber technologies, which have strategic impacts on various dimensions of social, cultural, economic, political, technological, security, and military-defense governance, require a comprehensive, structured, and cohesive approach to protect and safeguard national interests and security. This approach aims to maintain oversight over events, trends, environmental changes, and developments, both current and future, to enable decision-making, planning, and management. This research examined the impacts of emerging cyber technologies on national security. In the first step, specific characteristics were analyzed to create a unique identity for emerging technologies as a unified essence with identifiable capabilities based on these characteristics. Initially, the specific attributes of the technologies were identified in seven main categories. Subsequently, in a more abstract mental space, independent of the ongoing updates in technology, the impacts on the dimensions of national security were examined, demonstrating that the various components describing technology have a direct effect on all diverse dimensions of national security. Therefore, from a national perspective, it is evident that endogenous strengthening of national power through proper management of emerging technologies will enhance influence over the desired geometry of the new world order. Proactive measures by the country's governance system, with an opportunity-driven approach against the threats posed by emerging technologies, hold significant strategic importance.

In response to the main research question (the impact of emerging cyber technologies on national security), it can be acknowledged that the characteristics of emerging technologies, in response to the first sub-question, are specifically categorized in Figure 2, followed by the relevant operational definitions. Additionally, by identifying the direct impact of each of the seven characteristics of technology on each dimension of national security in the second sub-question, the answer to the first question is presented as follows: the political-security dimension shows the highest susceptibility, followed by military-defense, socio-cultural, and economic dimensions in subsequent ranks. However, due to the small numerical differences in the average scores assigned to each dimension, it

can be said that emerging technologies have a direct and meaningful impact on all dimensions of national security. Through statistical analysis and the summary of relationships between the variables based on the results presented in this research, the impacts can be elucidated as follows:

In the first rank, data-driven intelligence, with a correlation coefficient of 0.563, has the highest direct and positive relationship with national security, with an impact rate of 31.9%, and its greatest impact is on the military-defense dimension of national security. In the second rank, complexity and spatial change, with a correlation coefficient of 0.414, have a direct and positive relationship with national security, with an impact rate of 17.3%, and their greatest impact is also on the military-defense dimension of national security. In the third rank, convergence and immersion, with a correlation coefficient of 0.411 and an impact rate of 17.1%, have a direct and positive relationship with national security, with their greatest impact on the military-defense dimension. In the fourth rank, distributedness and ubiquitous perception, with a correlation coefficient of 0.369 and an impact rate of 13.9%, have a direct and positive relationship with national security, with the greatest impact on the political-security dimension. In the fifth rank, sharing and social participation, with a correlation coefficient of 0.366 and an impact rate of 13.7%, have a direct and positive relationship with national security, with the greatest impact on the political-security dimension. In the sixth rank, scale development, with a correlation coefficient of 0.344 and an impact rate of 12.1%, have a direct and positive relationship with national security, with the greatest impact on the military-defense dimension. In the seventh rank, threat generation, with a correlation coefficient of 0.303 and an impact rate of 9.3%, have a direct and positive relationship with national security, with the greatest impact on the political-security dimension.

Suggestions

Given the fluid and transformative nature of cyberspace, which is significantly dependent on the growth of science and technology, particularly due to the convergence and integration of various technological domains, it possesses a high level of complexity and uncertainty, along with rapid and profound changes unprecedented in human experience. Therefore, to safeguard against its threats and to take advantage of unparalleled opportunities, as well as to convert threats into opportunities with strategic depth in the realm of national cyber governance, it is hereby suggested to establish a specialized and

knowledge-based mechanism for continuous monitoring and ongoing ontology aimed at understanding the changing nature of cyberspace in the country. This would ensure resilience against strategic surprises at the national level and maintain agility and proactive capability for national cyber governance, specifically within each governing organization, particularly in the security domain.

With the introduction of the definitive impacts of technology on the dimensions of national security, for doctoral studies, research related to the formulation of a "National System for the Governance of Emerging Technologies Based on Islamic-Iranian Values and Principles" should include deep and continuous ontology, identification of major needs and issues within the country, vision, overarching goals, national ecosystem architecture for technology, executive policies, institutional mapping, relationships among actors, formulation of proactive measures at all national and transnational levels, and definition of the logical task structure for the pillars of national governance.

Additionally, it is recommended that the impacts of emerging cyber technologies be specifically examined in each dimension of national security—including economic, political, cultural, social, military, environmental, legal, and judicial—individually and with a more specialized and clearer perspective. Strategic proactive measures should be provided to the custodians and managers of those areas to leverage opportunities and mitigate threats.

"Strategic Model for Preserving Ethics and Culture in the Era of Cyber Transformations Influenced by Emerging Technologies," as well as "Designing a System of Responsibility and Accountability" in this era are other proposed research topics at the national level.

Considering the importance of international relations and the reciprocal effects of foreign policy on the development of emerging cyber technologies at both national and global levels, the requirements, architecture, and institutional mapping of the country's cyber diplomacy system within the Ministry of Foreign Affairs should be studied with a Headquarters perspective (defining the roles and positions of all actors in the economic, scientific, technological, educational, cultural, security, defense, legal, and judicial domains) as part of a national system, as a doctoral dissertation titled "Strategic Model for the Country's Cyber Diplomacy System."

The results of this research should be made available to stakeholders and custodians of security and military affairs in the country, so they can be utilized in national planning. Furthermore, the risks arising from adversaries' use of modern cyber technologies and the potential for optimal utilization of these technologies to enhance national security should not be overlooked.

References

Persian References

1. Khamenei, S. A. (2021). Statements in a meeting with members of the Assembly of Experts. 19/03/2022.
2. Izadi, J., & Takbiri, M. (2014). The impact of smart diplomacy on political communication in the international system. Volume 7, Issue 26, 34-55.
3. Bahoush Fardaghi, M. (2017). Examining the concept or metaphor of national security in constructivist theory. Political Science Quarterly, 4(14), 101-112.
4. Bakhshi Taliyabi, R., Azarshab, M. T., & Najm Abadi, M. (2017). The role of security in the Copenhagen School: A framework for analysis. Specialized Journal of Political Science, 13(40), 119-146.
5. Bayat, B. (2019). Theories of national security. Strategic Publications Center of the University and National Defense Research Institute, Tehran, 375 pages. Dewey classification: 355.03.
6. Pishgahi-Fard, Z., Hosseini, S. M., & Farahani, M. (2014). Ranking the national power of Middle Eastern countries using compensatory multi-criteria decision-making. Journal of Geographical Research, 2(5), 1-44.
7. Khani, M. (2020). Conceptualizing security crises with an emphasis on the teachings of the Copenhagen School. Strategic Environment Quarterly, 4(12), 85-102.
8. Kohansal Kolkanari, M., & Babaei Nasami, A. (2017). Cybersecurity: Threats and their impacts on national security. In Proceedings of the Second International Congress on Humanities and Cultural Studies.

9. Mahmoudzadeh, E. (2010). Managing the future with tomorrow's technology. Publisher: Institute of Iran Language, Persian. Dewey classification: 658.4, 3rd edition, 1000 copies printed.
10. Moradi, A., Ramazani, M., Mohammadi, H., & Jahangiraki, A. (2020). National security in the new era: Trends and components. Strategic Publications Center of the National Defense University, Tehran. ISBN: 978-622-248-205-3, first edition.
11. Helili, K., Valavi, M. R., Mohammadi Sefat, M. R., & Bagheri, M. (2018). Cyber power based on a fractal approach and its impact on national security in cyberspace. National Security Quarterly, 8(29), 173-200.
12. Hendiani, A. (2007). Examining conceptual transformations of security in the security environment. Administrative *Science,* 9(3), 9-30.

English References

1. Andrade, Roberto O and Yoo, Sang Guun;(2019), Cognitive security: A comprehensive study of cognitive science in cybersecurity, Journal of Information Security and Applications, 48, 102352, www.elsevier.com/locate/jisa
2. Attiah, Mark A. and Farah, Martha J. (15 May 2014), Minds, motherboards, and money: futurism and realism in the neuroethics of BCI technologies. Frontiers in Systems Neuroscience. 8 (86): 86. doi:10.3389/fnsys.2014.00086.,
3. Atlam, Hany F.; Alenezi, Ahmed; Alassafi, Madini O.; Wills, Gary B.; (June 2018), Intelligent Systems and Applications, Blockchain with Internet of Things: Benefits, Challenges, and Future Directions, I.J., 40-48 Published Online in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijisa.2018.06.05
4. Billingsley, Joseph L.; (May 2023), Integrated Deterrence and Cyberspace Selected Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest, National Defense University Press Washington, D.C. First printing.
5. Brain, David Johnson; Alida, Draudt; Brown, Jason C.; Lieutenant Colonel Robert, J. Ross; (2020), INFORMATION WARFARE AND THE FUTURE OF CONFLICT, Arizona State University.
6. Breno, Pauli Medeiros and Luiz, Rogério Franco Goldoni; (Jan/Apr 2020), The Fundamental Conceptual Trinity of Cyberspace, Contexto Internacional vol. 42(1), Brazillian Army Command and

General Staff College (ECEME), PP:31-54 http://dx.doi.org/10.1590/S0102-8529.2019420100002

7. Bussu, Sonia; Yaron, Golan; Hargreaves, Anna; (2022), Understanding developments in Participatory Governance A report on findings from a scoping review of the literature and expert interviews, Manchester Metropolitan University, 72 pages. ISBN: 9781910029787
8. Cadell, Last; (2020), Global Brain Singularity-Universal History, Future Evolution and Humanity's Dialectical Horizon, Springerm Vrije Universiteit Brussel Brussels, Belgium, 339 pages. ISBN 978-3-030-46966-5
9. Cheraghi, Ahmad Reza; Shahzad, Sahdia; Graffi, Kalman; (2021), Past, Present, and Future of Swarm Robotics, University D¨usseldorf, Germany, published in Intelligent Systems Conference (IntelliSys 2021).
10. Chisnall, Mick; (2020), Digital slavery, time for abolition?, POLICY STUDIES, VOL. 41, NO.5, Taylor & Francis Group. UK Limited, pp: 488–506. https://doi.org/10.1080/01442872.2020.1724926.
11. Cozzens, Susan; Sonia, Gatchair; Jongseok, Kang; Kyung-Sup, Kim; Hyuck, Jai Lee; Gonzalo, Ordóñez & Alan, Porter; (2010), Emerging technologies: quantitative identification and measurement, Technology Analysis & Strategic Management, 22:3, 361-376, DOI: 10.1080/09537321003647396.
12. Dotsenko, Elena; (2017), The Second International Innovative Mining Symposium, NBIC-Convergence as a Paradigm Platform of Sustainable Development, E3S Web of Conferences 21, 04013, Plekhanov Russian University of Economics, Moscow, DOI: 10.1051/e3sconf/20172104013.
13. Dwivedi, Yogesh K.; Laurie, Hughes; Baabdullah, Abdullah M.; Ribeiro-Navarrete, Samuel; et al.; (2022), Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, International Journal of Information Management, 66, doi:10.1016/j.ijinfomgt.2022.102542.
14. EU (European Union) (2019), European Cluster and Industrial Transformation Trends Report, European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Unit F.2: Clusters, Social Economy and Entrepreneurship, Luxembourg: Publications Office of the European Union, scientific supervision: Ron Boschma (Utrecht University), ISBN 978-92-9202-747-6.

15. Fei, Hu; Xin-Lin, Huang and DongXiu, Ou; (2021), UAV Swarm Networks: Models, Protocols, and Systems, CRC press, ISBN: 9781003039327 (ebk)
16. Fernando, Marie D; (2019), The Phenomenon of Social Computing, A Thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy, Western Sydney University.
17. Gompert, David C. and Binnendijk, Hans; (2016), The Power to Coerce: Countering Adversaries Without Going to War, Prepared for the United States Army, Published by the RAND Corporation, www.rand.org/t/rr1000
18. Halaweh, Mohanad; (2013), Emerging Technology: What is it?, ISSN: 0718-2724. (http://www.jotmi.org) Journal of Technology Management & Innovation © Universidad Alberto Hurtado, Facultad de Economía y Negocios, J. Technol. Manag. Innov. 2013, Volume 8, Issue 3, 108-115.
19. Huansheng, Ning; (2022), A Brief History of Cyberspace, 227 pages, CRC Press, Taylor & Francis Group, ISBN: 978-1-003-25738-7
20. Huansheng, Ning; Xiaozhen, Ye; Bouras, Mohammed Amine; Dawei, Wei and Daneshmand, Mahmoud; (June 2018), General Cyberspace: Cyberspace and Cyber-enabled Spaces, IEEE INTERNET OF THINGS JOURNAL, VOL. 5, NO. 3, 2327-4662 (c), DOI 10.1109/JIOT.2018.2815535, IEEE, .1843-1856.
21. JP, Joint Publication 3-12 Cyberspace Operations, (5 February 2013) U.S. Army, and so updated: 8 June 2018.
22. Kademi, Anas Maazu and Koltuksuz, Ahmet Hasan; (2021), Cyber-physical-socialinformation- thinking hyperspace: a manifold of cyberspatial entities, Computer Engineering Department, Yasar University, Izmir, Turkey, https://www.emerald.com/insight/0368-492X.htm
23. Kademi, Anas Mu'azu and Koltuksuz, Ahmet; (December 2020), Dynamic Cyberspace Modeling from Network Automata, IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.12, doi:10.22937/IJCSNS.2020.20.12.4
24. Lee, Young-Chul and Moon, Ju-Young; (2020), Introduction to Bionanotechnology, Springer Nature Singapore Pte Ltd., 242 pages, ISBN 978-981-15-1293-3
25. Meijer, AJ; Lips, M. and Chen, K; (2019), Open Governance: A New Paradigm for Understanding Urban Governance in an Information Age. Front. Sustain. Cities 1:3. doi: 10.3389/frsc.2019.00003
26. Metcalfe, J. S.; (February 1995), Technology systems and technology policy in an evolutionary framework, Cambridge Journal

of Economics Vol. 19, No. 1, Special Issue on Technology and Innovation, Published By: Oxford University Press, 25-46.

27. Montasari, Reza; Hill, Richard and Parkinson, Simon; (April-June 2020), Digital Forensics: Challenges and Opportunities for Future Studies, University of Huddersfield, Huddersfield, UK, International Journal of Organizational and Collective Intelligence Volume 10 • Issue 2, IGI Global.
28. Novikov, D.A.; (2016), Cybernetics From Past to Future, Switzerland, Springer, 115 PAGES. ISSN 2198-4182
29. Ogechukwu, iloanusi; Uche, nnolim and Edwin, umoh; (February 2020), Chaos Theory and Solution Models for National Security, Nigerian Defence Academy (NDA) International Conference on State and Security Kaduna, Nigeria, 24th – 26th
30. Priyadarshini, Ishaani and Cotton, Chase; (2020), Intelligence in cyberspace: the road to cyber singularity, JOURNAL OF EXPERIMENTAL & THEORETICAL ARTIFICIAL INTELLIGENCE https://doi.org/10.1080/0952813X.2020.1784296
31. Reding, Dale F.; Álvaro, Martín Blanco; Angelo, De Lucia; Col Laura, A. Regan and Daniel, Bayliss; (2023), Science & Technology Trends 2023-2043 Across the Physical, Biological, and Information Domains VOLUME 2: Analysis, NATO Science & Technology Organization.
32. Roco, Mihail C.; (2020), Principles of convergence in nature and society and their application: from nanoscale, digits, and logic steps to global progress, Journal of Nanoparticle Research, doi.org/10.1007/s11051-020-05032-0, Springer, mroco@nsf.gov, Collection on Nanotechnology Convergence in Africa, National Science Foundation and National Nanotechnology Initiative, Arlington, VA, USA.
33. Rotolo, Daniele; Hicks, Diana and Martin, Ben R.; (January 5, 2016), What Is an Emerging Technology? DOI: 10.1016/j.respol.2015.06.006. publication in "Research Policy", 44 pages. Available at: www.sussex.ac.uk/spru/swps2015-06, SPRU – Science Policy Research Unit, University of Sussex.
34. Ryan, Mark; (2020), The Future of Transportation: Ethical, Legal, Social and Economic Impacts of Self-driving Vehicles in the Year 2025, Springer, Science and Engineering Ethics, 26:1185–1208 https://doi.org/10.1007/s11948-019-00130-2 University of Twente, Enschede, The Netherlands
35. Schmidt, Nikola; (2016) The Birth of Cyber as a National Security Agenda, Ph.D. Thesis, Faculty of Social Sciences Charles University Prague, Czech Republic

36. Schwab, Klaus; (2016), The Fourth Industrial Revolution, World Economic Forum, ISBN-10: 1944835016
37. Scott Kevin D., (2018), Joint Publication 3-12 Cyberspace Operations, JP3-12.
38. Stahl, Bernd Carsten; (June 2011), What Does the Future Hold? A Critical View of Emerging Information and Communication Technologies and Their Social Consequences, Chapter in IFIP Advances in Information and Communication Technology, DOI: 10.1007/978-3-642-21364-9_5
39. Theiner, Patrick; Schwanholz, Julia & Busch, Andreas; (2017), Parliaments 2.0? Digital Media Use by National Parliaments in the EU, pp:77-96, Managing Democracy in the Digital Age Internet Regulation, Social Media Use, and Online Civic Engagement, Springer. DOI 10.1007/978-3-319-61708-4_5
40. Tidjon, Lionel and Khomh, Foutse; (2022), Never trust, always verify a roadmap for Trustworthy AI, DGIGL, Polytechnique Montr´eal Montr´eal, QC H3C 3A7, Canada,
41. TREVOR, JOHNSTON; TROY, D. SMITH and J. LUKE, IRWIN; (2018), ADDITIVE MANUFACTURING IN 2040, Powerful Enabler, Disruptive Threat, Security 2024, RAND Corporation
42. Yong-Woon, KIM; Sangkeun, YOO; Hyunjeong, LEE and Soonhung, HAN; (2021), “Characterization of Digital Twin”, National AI Research Institute,
43. Zachary, D. Clopton; (2016), "Territoriality, Technology, and National Security," 83 University of Chicago Law Review 45. https://scholarship.law.cornell.edu/facpub/1624/,45-63.