

National Cybersecurity: A New Evolving Concept

الأمن السيبراني الوطني: مفهوم جديد آخذ في التطور

Badreddine BOUKARRITA*

University of Jijel (Algeria)

b.boukarrita@univ-jijel.dz

Date of send:19/04/2025 Date of acceptance:28/05/2025 Date of publication ;04/06/2025

Abstract

The growing complexity and frequency of cyber threats have made national cybersecurity a fundamental pillar of modern security frameworks. Now, governments must redefine defense strategies to address espionage, cyber warfare, and infrastructure disruptions. Using securitization theory and threat politics, this study examines the institutionalization of cybersecurity, illustrating its evolution from a technical safeguard to a geopolitical necessity. The findings reveal that AI-driven attacks, vulnerabilities in quantum computing, and cyber militarization have reshaped security priorities, prompting investments in encryption, AI-powered threat detection, and cyber deterrence strategies. The study underscores the necessity of international cooperation, emphasizing the importance of multinational intelligence sharing, regulatory harmonization, and coordinated cybersecurity governance. As digital systems become integral to governance, economic stability, and military operations, nations must adopt proactive cybersecurity policies to ensure sovereignty and resilience. Cybersecurity is ultimately a dynamic and evolving domain that requires continuous adaptation to counter emerging threats.

Keywords: Cybersecurity, National Security, Cyber Threats, Cyberspace.

* *Corresponding author*

Introduction

The evolution of the internet and social media has been instrumental in the paradigm shift towards a globalised information exchange, resulting in the rapid dissemination of information on a worldwide scale and the substantial expansion of the scope of data exchange. This transformation has actualised Marshall McLuhan's 1960s concept of the "Global Village". The advent of the digital revolution has engendered the development of a parallel virtual dimension that replicates and extends traditional societal functions, existing alongside our physical reality. It is evident that almost every conventional activity now has a digital counterpart, thereby giving rise to new paradigms such as e-governance, e-commerce, and e-learning. Concurrently, this development has introduced novel challenges, including cybercrime and cyber warfare. This digital representation of society has fundamentally reshaped human interaction, economic transactions and political processes in the 21st century.

Building on this foundation, the paper analyzes cybersecurity as a paramount national security challenge emerging from today's interconnected and rapidly evolving digital landscape. The investigation focuses on three critical dimensions: the expanding ecosystem of cyber actors, their proliferating strategic interests, and the resulting conflicts in this contested domain. The study addresses the following core research question:

How and why have cyber threats emerged as a fundamental challenge to national security?

In order to address this question, the present paper adopts a conceptual and analytical approach, situating cybersecurity within the broader framework of national security. The analysis draws on theoretical perspectives from security studies, including realism, securitization theory and threat politics, to demonstrate how security paradigms have expanded in response to evolving cyber threats. The study employs qualitative methods to complement this framework, examining historical cases, expert analyses, and government strategies to demonstrate cybersecurity's shift from a technical issue to a core national security priority. Collectively, these approaches furnish a systematic evaluation of the expanding significance of cybersecurity within the realms of governance and defence.

The paper is structured around three key themes:

Firstly: Understanding Cybersecurity: Core Concepts and Connections

Secondly: Expanding the concept of security and the emergence of cybersecurity.

Thirdly: Cyber threats as a national security issue.

Fourthly: from "cybersecurity" to "national cybersecurity"

Firstly: Understanding Cybersecurity: Core Concepts and Connections

Cybersecurity can be defined as a comprehensive discipline encompassing a wide array of technologies, policies, and risk management strategies. The overarching aim of this field is to secure digital environments and protect organisational assets. The International Telecommunication Union (ITU) defines it as “the collection of

safeguards, best practices, and governance frameworks designed to maintain confidentiality, integrity, and availability across cyberspace”.¹ In a similar vein, Gregg Lindemulder and Matt Kosinski of the IBM Corporation (2024) characterise cybersecurity as the implementation of “technologies, practices and policies for preventing cyberattacks or mitigating their impact. These practices are designed to protect computer systems, applications, devices, data, financial assets and people against ransomware and other malware, phishing scams, data theft and other cyberthreats.”² Meanwhile, The International Organization for Standardization (ISO) defines cybersecurity as a risk management approach focused on "managing information security risks when information is in digital form in computers, storage and networks".³

The formulation of National Cybersecurity Strategies (NCSS) by governments typically begins by emphasizing the protection of information, computer security measures, or information assurance needs. While these terms are often used interchangeably, they represent distinct security domains. Information security focuses on protecting data regardless of format (digital, physical, etc.), whereas computer security ensures system availability and functionality, primarily focusing on infrastructure rather than data content. Information assurance involves assessing information protection needs based on sensitivity and strategic value. Despite their nuanced differences, all three principles align in pursuing confidentiality, integrity, and availability in cyberspace. Moreover, most unauthorized breaches of these principles are criminalized under national laws, highlighting cybersecurity’s growing regulatory importance.⁴

The field of cybersecurity has evolved beyond its original technical purview, becoming a strategic imperative for national security and economic resilience. In the contemporary context, cybersecurity frameworks have evolved to encompass critical concerns such as digital sovereignty, infrastructure security, and regulatory compliance. This evolution is evidenced by the diverse approaches adopted by National Cybersecurity Strategies (NCSS). This expansion underscores the growing recognition of cyberspace as a contested domain where threats to economic stability, democratic institutions, and military security intersect. The International Organization for Standardization (ISO) places significant emphasis on risk management in the digital domain, aligning with the International Telecommunication Union's (ITU) perspective on systematic cybersecurity governance. Collectively, these entities emphasise the dualistic nature of cybersecurity, illustrating it as both a technical safeguard and a governance challenge that necessitates continuous adaptation to emerging threats, including AI-driven cyberattacks and vulnerabilities introduced by quantum computing.⁵

In the realm of digital security, the field of cybersecurity has emerged as a predominant concern. However, it is imperative to recognise the emergence of several related concepts that have gained prominence in shaping digital security strategies. Foremost among these concepts is cybercrime, which the Encyclopedia Britannica defines as "the use of computer systems and digital networks to commit

illegal acts, including fraud, identity theft, and privacy violations"⁶. While fundamentally an extension of conventional criminal conduct, cybercrime presents distinctive challenges stemming from its transnational character, which complicates law enforcement efforts and jurisdictional coordination. Contemporary cybersecurity frameworks are progressively incorporating comprehensive measures to prevent and counteract cybercriminal operations, highlighting the growing interdependence between cybersecurity protocols and legal governance structures. This evolution reflects the necessity for adaptive approaches that address both technological vulnerabilities and regulatory frameworks in our increasingly digitalized world.

Although traditionally tied to military operations, cyber defence has become a vital pillar of cybersecurity, addressing threats ranging from criminal activities to espionage. The North Atlantic Treaty Organization (NATO) distinguishes cyber defence—defined as the proactive protection of operational Communications and Information Systems (CIS) against cyber threats—from broader information security (CIS security), which focuses on safeguarding data confidentiality, integrity, and availability. This distinction underscores cyber defence's role as a specialized subset of cybersecurity, ensuring resilience for national and organizational digital infrastructures. As cyberspace grows more contested, integrating cyber defence strategies with comprehensive cybersecurity frameworks is essential to defending critical systems, maintaining stability, and countering evolving threats.⁷

Cyber espionage has also become an increasingly strategic concern, particularly as nations increasingly exploit digital vulnerabilities to gain intelligence advantages. In contradistinction to conventional espionage, the practice of cyber-enabled intelligence gathering is characterised by an inherent level of anonymity, a factor that engenders complexity in terms of attribution and response measures. It is an established fact that governments and corporations are frequently the victims of cyber espionage operations. The objective of such operations is the extraction of sensitive data, trade secrets and national security intelligence. As digital infrastructures become increasingly integral to global economies, the potential for cyber espionage to reshape power dynamics is evident, with nations competing for technological supremacy through covert cyber operations. The indistinct demarcation between cyber espionage and cyber warfare gives rise to a series of ethical and legal dilemmas concerning the permissible boundaries of state-driven cyber activities.⁸

Another closely related concept to cybersecurity is cyber warfare. While no universally accepted definition exists, prevailing consensus describes it as state-sponsored or adversarial operations aimed at disrupting digital systems to achieve strategic objectives. Notably, military doctrines in countries like Russia and China have increasingly integrated cyber capabilities, emphasizing their use for destabilizing adversaries without conventional military engagement. The legal status of cyber warfare remains hotly debated, particularly regarding its classification under international law. As cyber conflicts grow more frequent, discussions about cyber norms, conduct frameworks, and deterrence mechanisms continue to shape the future of cybersecurity governance at national and global levels.⁹

This conceptual analysis demonstrates that cybersecurity has evolved from its technical origins into a comprehensive strategic paradigm encompassing four critical dimensions: cybercrime prevention (combating digital offenses against individuals and organizations), cyber defense (protecting critical infrastructure), counter-espionage (thwarting intelligence theft), and cyber warfare deterrence (safeguarding national security). In order to address these complex challenges, contemporary cybersecurity operates through three interdependent governance pillars: regulatory compliance (legal frameworks), intelligence coordination (threat detection), and holistic security strategies (resilience building). In the contemporary threat landscape, characterized by the proliferation of AI-powered attacks and vulnerabilities in quantum computing systems, the efficacy of cybersecurity measures necessitates the integration of advanced technological solutions, such as advanced encryption techniques, with a comprehensive risk management framework that aligns with ISO standards. The National Cybersecurity Strategies (NCSS) have evolved to reflect this multidimensional approach, acknowledging cyberspace as a domain where technological protection, legal accountability, and geopolitical stability intersect. In essence, contemporary cybersecurity can be regarded as both a technical safeguard and a strategic imperative. It necessitates continuous advancement in policy frameworks, international cooperation, and defensive capabilities to ensure the security of digital ecosystems against evolving threats.

Secondly: Expanding the Concept of Security and the Emergence of Cybersecurity

Realists based their perception of national security on conflicts of interest between states in a world without a central authority to regulate international relations. Conflicts of this nature frequently result in warfare, which is predominantly resolved through the utilisation of military force. Consequently, realists viewed security as deriving from state power, with states seeking to ensure their security through self-reliance – a principle referred to by classical realists as 'self-help'. However, this perspective restricts the concept of security to military power, rendering it virtually synonymous with military security.

The realist perspective described above was closely aligned with the Cold War era, when threats were directly tied to military capabilities. During this period, the power of a state was measured by the aggregate of its military, economic, technological, and diplomatic resources. The distribution of these capabilities, which was both unequal and subject to change, determined the balance of power among states. However, in the aftermath of the Cold War, a new series of theoretical debates emerged, advocating for an expanded security agenda. This transition was precipitated by the emergence of non-military threats, a significant proportion of which emanated from non-state actors. These developments exposed the limitations of the traditional military-centric security framework and necessitated its broadening. The Copenhagen School became one of the most influential proponents of this revised approach.

In his seminal work, *'People, States, and Fear: The National Security Problem in International Relations'* (1983), Barry Buzan, the leading theorist of the Copenhagen School, reconceptualized security by moving beyond realist assumptions that prioritized military dimensions and state-centric approaches. He proposed a more comprehensive definition of security as “the pursuit of freedom from threat,” thereby expanding its scope to incorporate political, economic, and social dimensions alongside traditional military concerns.

The definition of security as “freedom from threat” suggests that security concerns emerge in response to existing threats. This standpoint is congruent with the institutionalisation of cybersecurity, as the proliferation of cyber threats endangers state security, necessitating an augmentation of security paradigms to encompass digital risks. Consequently, cybersecurity has evolved into a distinct security sector, reflecting the increasing necessity for structured frameworks that safeguard critical infrastructure and sensitive information. This transition signifies the evolution of cybersecurity from its technical origins, signifying its transformation into a strategic imperative within national security policies.

For instance, the Netherlands adopted a more expansive definition of cybersecurity, characterising it as “freedom from danger or damage due to the disruption, breakdown, or misuse of ICT”.¹⁰ This standpoint recognises cybersecurity not solely as a defence against external threats but also as a mechanism for ensuring the availability, reliability, and integrity of digital systems. The risks associated with ICT disruptions, including but not limited to data breaches, system failures and compromised confidentiality, serve to reinforce the notion that cybersecurity governance must be subject to continuous adaptation in order to counteract the emergence of new vulnerabilities. As digital infrastructures become increasingly entrenched within the economic, political and military spheres, cybersecurity has emerged as a pivotal element in ensuring national stability, mitigating threats posed by artificial intelligence (AI), and preparing for future challenges, such as vulnerabilities associated with quantum computing.

In late February 2002, Richard Clarke — cybersecurity advisor to President Bush and White House director of cybersecurity — and 54 computer scientists sent a letter to the president warning of the grave risk of a major cyberattack on America — one that “could devastate the national psyche and economy more broadly than did the September 11th attack”. The scientists highlighted that “critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense and the Internet, is highly vulnerable to cyber attack”¹¹. These warnings referred to a 'new' kind of threat to national security commonly known as 'cyber threats'. Such threats generally denote the malicious use of information and communication technology (ICT) by a diverse range of actors.

The state's integration into cyberspace through its various institutions has resulted in the emergence of new dimensions to its sovereign boundaries. While conventional discourse has historically centred on the securing of land, sea and air, the notion of securing cyberspace has emerged as a political topic among state

policymakers. This subject was formerly the domain of information systems and network security experts. As Richard Clarke astutely notes: “In the past, you would count the number of bombers and the number of tanks your enemy had. In the case of cyber war, you really can't tell whether the enemy has good weapons until the enemy uses them”.¹²

In their letter to President Bush, Clarke and his colleagues further stated: “We look to you, as America's leader, to act on behalf of the nation. Your conscientious and effective defense of our physical homeland should extend into the increasingly vital frontier of U.S. cyberspace. We anticipate that the nation will fully endorse and even expect this forward-thinking and courageous action in the face of such a major threat to national security.”¹³

This observation underscores cyberspace's ascendant role in national security. Clarke and his colleagues advocate for proactive governance to mitigate vulnerabilities in the digital domain, emphasising the inextricable link between physical and virtual security. The call to action asserts that cyberspace constitutes a vital component of national defence, thus necessitating the implementation of robust protective measures. This paradigm is indicative of the growing centrality of cybersecurity in preserving national interests and ensuring resilience against evolving threats.

As this section concludes, it becomes evident that cybersecurity has emerged as an essential extension of security theory, reflecting the transition from traditional, military-centric perspectives toward a broader, multidimensional framework. The increasing prominence of cyberspace as a sovereign domain has necessitated a reevaluation of national security strategies, integrating cybersecurity into the protection of critical infrastructure, digital assets, and geopolitical stability. The increasing institutionalization of cybersecurity, driven by escalating cyber threats, demonstrates how digital risks have profoundly reshaped security paradigms. This has led to a necessity for governments and organizations to adopt comprehensive governance models and proactive defense mechanisms. In light of the increasing prevalence of AI-driven attacks and vulnerabilities in quantum computing systems, the field of cybersecurity is poised to undergo significant advancements, thereby underscoring its role as a fundamental component of resilience and strategic security in the contemporary digital era, characterized by interdependence and interconnected systems.

Thirdly: Cyber Threats as a National Security Issue

Cyber threats are of a unique nature, occupying a nexus between multiple disciplines, including but not limited to computer science, information technology, the information revolution, and security studies. However, the field of international relations has been notably slow to engage with information and communication technologies, particularly the great challenges introduced by the digital revolution. As state involvement in cyberspace intensifies and security threats proliferate, these technological considerations have assumed growing prominence on national security agendas in recent decades.

In her book *Cybersecurity and Threat Politics: The American Efforts to Secure the Information Age* (2007), Myriam Dunn Cavelty employs the 'threat politics' approach to describe the political processes through which threats are transferred, removed from the political agenda or reshaped within it.¹⁴ The author employed this approach to address the question of how and why cyber threats have become one of the fundamental security challenges of the modern era.

In a parallel theoretical approach, Marek Górká (2023) applies securitisation theory to analyze cybersecurity policy in his seminal work '*Conceptualising Securitisation in the Field of Cybersecurity Policy*'. His framework posits that nation-states strategically seek to regulate cyberspace to align digital content with both domestic political agendas and foreign policy objectives. Building on Ulrich Beck's (2006) risk society paradigm, Górká demonstrates how states instrumentalize cybersecurity discourse to frame digital threats as existential risks, thereby justifying cyberspace securitization as a national security priority.¹⁵

The exponential growth of information and communication technologies (ICTs) has generated transformative societal benefits, but concurrently created an evolving landscape of sophisticated security challenges. Contemporary cyber threats demonstrate unprecedented heterogeneity, increasingly compromising the operational effectiveness of national security architectures. These systemic vulnerabilities now permeate foundational societal structures through multiple attack vectors, from economic cybercrimes and state-sponsored espionage to cyberterrorism and critical infrastructure attacks, each representing a potential catalyst for large-scale national security emergencies.¹⁶ This empirical evidence underscores the complex interdependence between cyberspace and national security.

It is evident that technological innovation engenders novel opportunities, yet concomitantly engenders multifarious security challenges. Contemporary threats, including cybercrime, digital espionage and infrastructure-targeted cyberattacks, have undergone a critical transformation. These threats have evolved from discrete technical anomalies to pressing strategic priorities. These evolving threats now directly compromise the functional integrity and strategic objectives of governmental institutions, societal structures, and economic systems.

From another perspective, the increasing interconnectedness of cyberspace has resulted in the blurring of traditional state boundaries, thereby rendering cyber threats, including cyberterrorism and infrastructure-targeted attacks, more tangible and transnational in nature. As states become increasingly integrated into the digital realm, their security vulnerabilities extend beyond physical borders, necessitating robust regulatory solutions and international cooperation. The pervasive nature of cyber risks has the potential to impact societal stability, governmental operations, and economic systems, thereby reinforcing the necessity for a comprehensive global cybersecurity framework.¹⁷ In consideration of the intricate nature of cyberspace, from which threats are emanating from distant actors and escalating rapidly, cybersecurity has evolved from being a domestic concern to a pivotal element of international security strategy.

To counter evolving cyber threats, nations must adopt a dual approach: strengthening internal cybersecurity resilience through advanced defense mechanisms while engaging in global intelligence-sharing and coordinated regulatory efforts to mitigate cross-border risks. The NATO CCDCOE framework (2012) emphasizes the need to align cybersecurity policies with national security priorities across political, strategic, operational, and technical domains, ensuring a cohesive response to cyber threats. To transition from reactive to proactive cybersecurity strategies, governments should promote multinational cooperation, thereby securing digital infrastructure while maintaining geopolitical stability in an increasingly interconnected world.¹⁸

Conversely, in order to address the increasingly serious issue of cyber security at the local level, it is essential that national security frameworks evolve to incorporate digital threats as fundamental security concerns rather than peripheral technical challenges. The NATO CCDCOE framework highlights the necessity of a multi-tiered cybersecurity strategy, ensuring alignment across the political, strategic, operational and technical domains. This structured approach enables governments to integrate cybersecurity into broader defence policies, thereby fortifying national resilience against increasingly sophisticated cyber threats.¹⁹ Adopting this model enables states to transition from reactive responses to proactive strategies that safeguard critical infrastructure, economic stability, and institutional integrity in an interconnected digital landscape.

It is imperative to recognise that cyber threats are not merely speculative concerns for the future; rather, they are pressing, immediate challenges that demand proactive strategies. In the contemporary geopolitical landscape, characterised by the evolution of national security, states are compelled to navigate a complex environment where both tangible and perceived risks influence policy decisions. The mounting prevalence of cyber threats, encompassing espionage and attacks on critical infrastructure, has firmly established their prominence on global security agendas, compelling substantial governmental investments in mitigation efforts despite the inherent uncertainties surrounding these threats.²⁰ Alexander Klimburg (2012) has identified several key dilemmas in the realm of cybersecurity policymaking, including the delicate balance between economic progress and security, the management of vulnerabilities in national infrastructure, the definition of public-private partnerships, and the reconciliation of data protection with intelligence-sharing imperatives. Furthermore, governments are obliged to address the challenge of safeguarding freedom of expression while maintaining political stability, ensuring that cybersecurity measures strengthen national security without undermining democratic principles.

In conclusion, the discourse on cyber threats underscores the critical need to balance proactive preparedness with adaptive strategies amid persistent uncertainty. As these threats continue to evolve globally, their integration into national security agendas demonstrates their enduring significance. Substantial government investments reflect the growing prioritization of cyber risks, marking a decisive

transition from theoretical analysis to concrete countermeasures against this escalating challenge.

Fourthly: from "cybersecurity" to "national cybersecurity"

The debates and revisions surrounding the concept of security as a whole, along with its expansion, can also be applied to cybersecurity. This field has also undergone re-evaluation and reform, informed by the aforementioned approaches of 'threat politics' and 'securitisation'.

Initial discussions about cyber threats focused primarily on the security of confidential or sensitive data. During the 1980s, hackers like Kevin Mitnick²¹ and John Draper²² gained notoriety through phone manipulation, or 'phreaking'²³, and later through computer hacking. Computer crimes, or offences committed with or against a computer, were a major concern at the time. However, despite being labelled as such, these issues had a national security dimension from the outset, as computer hacking was often successfully linked to foreign intelligence threats.²⁴

Consequently, while an implicit connection existed between early cybersecurity concepts and national security, this relationship remained ambiguous and failed to elevate cybersecurity to a national security priority—unlike its current status. During that era, the issue was predominantly the domain of computer engineers and technical specialists.

Since the early 1990s, following the conclusion of the Cold War, analysts have predicted that cyber warfare would become a defining feature of 21st-century conflict. Nevertheless, more than two decades later, individual hackers, foreign intelligence agencies, and criminal groups continue to represent the most significant threat in cyberspace. In 2008, during Russia's invasion of Georgia, a cyberattack accompanied the military operation. As Russian tanks and aircraft advanced into Georgian territory, cyber warriors targeted the Georgian Ministry of Defense. While the impact of this attack was negligible, it served as a cautionary indication that future confrontations would manifest in both the physical and virtual domains.²⁵

In recent years, the advent of individuals and companies into cyberspace has given rise to new industries and a vibrant social space, which has become an integral part of our daily lives. Concurrently, individuals, groups, and even governments began leveraging cyberspace to advance their own agendas by engaging in activities that inflict harm upon others. Terrorist groups employ the internet to recruit, train, and target their activities; organized criminal organizations leverage financial data to generate profits that exceed those from drug trafficking; and non-state actors, intelligence agencies, and militaries increasingly infiltrate information technology networks for espionage and to exert influence.

This trend is likely to persist as governments search for new methods and strategies to defend their interests in cyberspace, while also developing offensive capabilities to compete in this domain. Consequently, the relationship between cybersecurity and national security will become even stronger.

The term 'militarization of cyberspace' denotes the convergence of cybersecurity and national security. Although cyberspace is a man-made domain, it has become an

operational sphere for military activities, akin to land, sea, air, and space. Unlike these heavily regulated domains, however, cyberspace remains accessible to anyone with internet connectivity. This accessibility creates unique security challenges, as cyber disruptions affect all users indiscriminately. For instance, malware targeting commercial infrastructure can simultaneously degrade connectivity for government networks, military systems, and civilian internet access.²⁶

In the context of warfare, the internet serves as both a means and a target for military forces. Former U.S. Deputy Secretary of Defense, William J. Lynn, emphasised the critical importance of information infrastructure for national defence, stating: “The command and control of our forces, the intelligence and logistics on which they depend, the weapons technologies we develop and field—they all depend on our computer systems and networks. Indeed, our 21st century military simply cannot function without them.”²⁷

In their analysis of the internet as a military domain, Mikael Wedlin and Erik Westring emphasise its dual role as both a tool and a target in modern warfare. The report emphasises the growing societal reliance on the internet for critical functions, including defence operations. The findings of the research indicate that intelligence gathering, influence campaigns, and covert military activities are increasingly dependent on cyberspace. This development serves to consolidate cyberspace's role as a pivotal arena in contemporary total defence.²⁸

This statement underscores the profound dependence of modern military operations on sophisticated information and communication systems. In an era where digital infrastructure is the backbone of defense capabilities, the security and resilience of these systems are as important as traditional weaponry. The interconnected nature of command, intelligence, logistics, and weaponry underscores the dual-edged nature of technology: it is both a force multiplier and a potential vulnerability. Therefore, safeguarding cyberspace is a cornerstone of national security strategy, reflecting a paradigm shift from physical domains to the digital battlefield of the 21st century. It is not merely an auxiliary concern.²⁹

In the United States, the Pentagon is concerned that its personnel may share excessive amounts of data on social media platforms such as Facebook, or post unfavourable images or videos on YouTube that could undermine its efforts. Furthermore, military personnel could steal classified information and leak hundreds of thousands of secret documents to websites such as WikiLeaks, posing a significant risk to national security. Such activities demonstrate the challenge of balancing openness in cyberspace with the necessity of safeguarding sensitive information — an issue that is becoming increasingly pertinent in contemporary cybersecurity strategies.³⁰

A similar perspective can be found in discussions about the risks posed by data breaches and leaks within defence organisations. For instance, the exposure of sensitive Pentagon data via cloud-based storage servers highlights the vulnerabilities involved in managing classified information. Such incidents are often caused by

inadequate security measures, such as weak passwords or outdated software, and highlight the urgent need for robust cybersecurity protocols.³¹

This highlights the significant vulnerabilities posed by the misuse of digital platforms and the resulting challenges for national security agencies. The combination of individual actions, such as oversharing on social media or leaking classified documents, with the accessibility of cyberspace demonstrates how the digital landscape can amplify risks to national security.³² As governments adapt to these emerging challenges, they must strike a delicate balance between enabling freedom of expression and protecting sensitive information. The growing complexity of this issue underscores the urgent need for robust cybersecurity policies, proactive education, and vigilance in both military and civilian contexts.

Unlike traditional fields of warfare, such as land, air, or sea, where governments hold sole power, cyberspace is a sensitive area of national security because governments do not hold sole power there. Instead, individuals can easily use technology to compete on a global scale. This trend of virtual democratisation is likely to continue, granting individuals a level of power that would have been unimaginable just a decade ago. Satellite imagery, for example, which was once highly classified and accessible only to the US intelligence community, can now be viewed by anyone using an iPhone with applications such as Google Earth. Similarly, while the complexity and high cost of producing nuclear weapons restricts their manufacture to governments, the same cannot be said for virtual weapons of mass destruction. These virtual tools have the power to devastate data and networks, undermine international credibility, and disrupt commerce. Malicious activities such as worms, viruses and botnets regularly cause disruption to internet operations, further highlighting the urgent need for robust cybersecurity measures to address these evolving threats.³³

The tangible impact of virtual activities on the physical world highlights the growing complexity of cybersecurity challenges. Activities such as online terrorist recruitment and training, disruption to communication systems, and interference with energy production demonstrate the wide range of threats that are emerging from cyberspace. Criminal groups use cyberspace to transfer funds, conceal identities, and coordinate operations, which makes it difficult for governments to counter these actions. Consequently, cyberspace is becoming an increasingly important focus for governments, which now view it as a strategic dimension within the broader framework of national security, not merely a technical domain. This shift underscores the evolving nature of modern threats and the urgent need for innovative strategies to address them.³⁴

This analysis aptly highlights the evolving relationship between cybersecurity and national security. The multifaceted nature of cyber threats, ranging from online recruitment to the disruption of critical infrastructure, emphasises the urgent need for governments to address these challenges with foresight and adaptability. As cyberspace becomes a strategic arena, the demand for innovative, coordinated

solutions is increasing, prompting discussions about the evolution of the concept of national cybersecurity in recent years.

In conclusion, the evolution of cybersecurity as a national security priority highlights its growing importance in protecting critical assets, digital infrastructure and sovereign interests. It has become a fundamental pillar of modern security strategies, reflecting the convergence of cyberspace with national defence, intelligence operations and geopolitical stability. As digital infrastructure becomes increasingly integrated into governmental, economic, and military systems, the threats posed by cyber warfare, espionage, and transnational cybercrime require a proactive and adaptive approach to securing critical assets. Governments now recognise that cybersecurity is a strategic imperative requiring comprehensive governance frameworks that integrate risk management, resilience-building and cyber deterrence measures, not merely a technical concern. This shift highlights the changing nature of national security. Cyberspace is now not only a domain of operations, but also a contested arena in which state and non-state actors engage in influence campaigns, intelligence exploitation and disruptive tactics. National cybersecurity can therefore be defined as the organised implementation of policies, technological safeguards and defensive strategies that aim to secure a nation's digital infrastructure, critical assets and sovereign interests against evolving cyber threats. This definition encompasses defensive and offensive considerations, ensuring the confidentiality, integrity and availability of national cyber environments, and addressing the geopolitical ramifications of cyber vulnerabilities. Given the increasing prevalence of AI-driven attacks, quantum computing risks and the militarisation of cyberspace, cybersecurity remains at the forefront of national security discussions. This requires continuous innovation, international cooperation and the development of resilient digital ecosystems to safeguard stability in an era of heightened cyber competition.

Conclusion

As the digital landscape continues to evolve at an unprecedented pace, cybersecurity has become a defining pillar of national security. It has expanded beyond technical safeguards to encompass strategic resilience, international cooperation and geopolitical stability. The development of cybersecurity, from an initial focus on data protection and cybercrime prevention to its current status as a national security priority, reflects a fundamental change in how states perceive and respond to cyber threats.

In today's interconnected security landscape, governments must address cyber warfare, espionage and transnational cybercrime as core national security concerns, not merely isolated technical challenges. This study shows that cyberspace has become an operational domain in which state and non-state actors carry out influence campaigns, exploit intelligence and use disruptive cyber tactics. This highlights the need for structured cybersecurity governance.

National cybersecurity can thus be defined as the organised implementation of policies, technological safeguards and defensive strategies that aim to secure a

nation's digital infrastructure, critical assets and sovereign interests against evolving cyber threats. This definition incorporates defensive and offensive considerations to ensure the confidentiality, integrity and availability of cyber environments, while also addressing the geopolitical implications of cyber vulnerabilities.

The study emphasised that AI-driven cyberattacks, quantum computing risks and the militarisation of cyberspace present increasingly sophisticated challenges. This requires continuous innovation in cybersecurity governance, resilience-building and deterrence strategies. As digital ecosystems become increasingly integrated into economic, political and military systems, it is crucial for nations to adopt proactive cybersecurity policies that ensure global cooperation and adaptive defence mechanisms, thereby preserving stability in an era of heightened cyber competition.

Ultimately, Hamadoun Touré's stark warning—delivered as Secretary-General of the International Telecommunication Union—that the next world war could erupt in cyberspace remains prophetic. History shows that war leaves no true victors, only collective devastation; thus, prevention is paramount. Given that cybercriminals operate transnationally, attacking multiple targets simultaneously without physical presence, only global collaboration can secure cyberspace effectively.

Upon concluding this article, the following findings have been established:

1. National cybersecurity has evolved from a technical safeguard into a strategic pillar of national security, addressing the protection of sovereign interests, critical infrastructure and geopolitical stability. Governments now recognise that cyberspace is a contested arena as well as an operational domain, necessitating comprehensive cybersecurity policies and deterrence strategies.

2. The securitisation of cyberspace has fundamentally reshaped national security paradigms by extending beyond traditional, military-focused strategies to recognise cyber threats as an existential risk. As cyber operations have become a key influence on economic stability, intelligence frameworks and defence postures, governments must adopt multi-tiered cybersecurity governance models to maintain national resilience.

3. Cyber threats have accelerated technological advancements in cybersecurity, driving investments in AI-powered threat detection, quantum-resistant encryption, and adaptive cyber risk mitigation frameworks. As adversaries develop more sophisticated attack methods, nations must continuously innovate their cybersecurity infrastructure to counteract AI-driven cyber warfare and secure digital assets.

4. Cyber warfare has changed the way global conflicts are fought, with cyberspace now being used for influence campaigns, intelligence operations and digital disruption strategies. As cyber capabilities are integrated into military doctrines, states must strike a balance between offensive cyber measures and defensive cybersecurity strategies in order to ensure operational security and mitigate the risk of international escalation.

5. International cooperation is essential in countering transnational cyber risks, which reinforces the need for multinational intelligence-sharing, policy harmonisation and collaborative cybersecurity frameworks. In an era of heightened

cyber competition, nations must prioritise strategic alliances and coordinated cybersecurity governance to preserve digital sovereignty and global security stability, given the borderless nature of cyber threats.

Footnotes

¹International Telecommunication Union (ITU), "Cybersecurity," accessed May 24, 2025, <https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx>.

²Gregg Lindemulder and Matt Kosinski, "Cybersecurity," IBM Think, accessed May 24, 2025, <https://www.ibm.com/think/topics/cybersecurity>.

³International Organization for Standardization (ISO), "ISO/IEC TS 27100:2020," accessed May 24, 2025, <https://www.iso27001security.com/html/27100.html>.

⁴Melissa Hathaway and Alexander Klimburg, "Preliminary Considerations: On National Cyber Security," in *National Cyber Security Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), p 8.

⁵Ibid, pp 8-9.

⁶Britannica, "Cybercrime," *Encyclopedia Britannica*, accessed May 10, 2025, <https://www.britannica.com/topic/cybercrime>.

⁷Melissa Hathaway and Alexander Klimburg, Op. cit, pp 12-13.

⁸Ibid, p16.

⁹Ibid, pp 17-19.

¹⁰Melissa Hathaway and Alexander Klimburg, Op. cit, p 12.

¹¹"a letter from concerned scientists", *PBS Public Broadcasting Service*, 27 February 2002, <https://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/letter.html>, accessed - January 18, 2025, 10:30 AM.

¹²"CYBER WAR!", *PBS Public Broadcasting Service*, 24 april 2003, <https://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html>, accessed - January 18, 2025, 09:30 AM.

¹³"a letter from concerned scientists", Op.Cit.

¹⁴Myriam Dunn Cavelty, *Cyber-security and threat politics: US efforts to secure the information age*. Routledge, 2007, p25.

¹⁵Marek Górka. "Conceptualising securitisation in the field of cyber security policy." *Journal of Modern Science* 53.4 (2023), p-p268-269.

¹⁶Imre Dobák. "Thoughts on the evolution of national security in cyberspace." *Security and Defence Quarterly* 33.1 (2021), p 76.

¹⁷Ibid, p77.

¹⁸Laszlo Kovacs, "National Cyber Security as the Cornerstone of National Security," *Land Forces Academy Review* 23, no. 2 (2018), p 114.

¹⁹Ibid, pp 114-115.

²⁰Myriam Dunn Cavelty, Op.cit, p6.

²¹Kevin David Mitnick, a computer scientist and cybersecurity consultant, is an American Jew who was one of the world's most prominent hackers during the 1980s and 1990s.

²²John Thomas Draper, an American computer programmer, is recognized as one of the most famous hackers and system infiltrators in the world.

²³"Phreaking" refers to hacking into telephone systems and other non-internet-connected devices. It originated in the mid-20th century as a practice among individuals who explored telecommunication systems, often to manipulate or bypass charges, using techniques like tone generation or system vulnerabilities. This term reflects an early form of hacking before the digital age fully emerged.

²⁴Myriam Dunn Cavelty, Op.Cit., p44.

²⁵ Derek S. Reveron, "An introduction to national security and cyberspace." In *Cyberspace and national security: Threats, opportunities, and power in a virtual world*, Georgetown University Press, Georgetown, 2012, p3.

²⁶ Ibid., p6.

²⁷ Ibid, p6.

²⁸ Mikael Wedlin and Erik Westring, "The Internet as a Military Arena: a Challenge for the New Total Defence", *Offprint from Strategic Outlook* 7, November 2017, pp 1-4, <https://www.foi.se/rest-api/report/FOI%20Memo%206206>, accessed - January 18, 2025, 10:00 AM.

²⁹ This perspective aligns with the idea that the internet is essential for military command, control and logistics, and for developing and deploying advanced weapon technologies. It emphasises that cyberspace is a strategic battlefield in its own right, not just a support system.

³⁰ Derek S. Reveron, Op.Cit., p7.

³¹ Brian Griffin, "Pentagon's Largest IT Servicer Rocked In Cyber Breach", *Triad Stage Spericorn*, July 24, 2024, <https://triad-stage.spericorn.com/blogs/pentagons-largest-it-servicer-rocked-in-cyber-breach/>, accessed - January 18, 2025, 11:30 AM.

³² Such breaches compromise national security and raise concerns about privacy and civil liberties, particularly when surveillance data includes innocent public posts by ordinary citizens. The challenge of protecting sensitive information while respecting individual rights is a problem that modern cybersecurity strategies must address.

³³ Derek S. Reveron, Op.Cit., p7.

³⁴ Ibid, p7.