Building Cyber Resilience to Face the Challenges of Cognitive Warfare

Raluca Radu
National Defense University, Romania

eralucaradu@gmail.com

Abstract: In the context of strategic ambiguity characterizing the geopolitical landscape of the past two years, cyber resilience plays a vital role in advancing alliances' deterrence and defense goals while minimizing the effects of cognitive warfare. The EU addresses cyber resilience by implementing mandatory cybersecurity requirements to ensure the development of secure digital products, significantly reducing vulnerabilities that impact businesses (EU, 2020; EU, 2022). In contrast, NATO prioritizes cybersecurity in the context of communication systems and information-sharing frameworks, while encouraging member states to bolster their cyber defense capabilities (NATO, 2024). However, the susceptibility of the human factor as a target of cognitive warfare conducted through cyberattacks is not explicitly addressed in international cybersecurity policies. This theoretical research aims to identify methods and tools to enhance cyber resilience in response to the challenges of cognitive warfare. Through the available literature, this paper establishes the conceptual framework for understanding cyber resilience and cognitive warfare. Using observation as a research method, we identified a series of similarities in NATO and EU programs and strategies targeting the cognitive dimension, including measures aimed at countering disinformation, fostering resilience against psychological manipulation, and enhancing information-sharing protocols among member states. While the Alliances remain at the forefront of cyber defence, there is still room for improvement. To enhance cyber and organizational resilience, Romania's specialized cyber defense structures employ strategies focused on raising civil society awareness, integrating adaptability into the education system, and fostering effective communication and collaboration both within and across public institutions. The key observation presented in this study is that a comprehensive approach to building cyber resilience is essential not only for enhancing deterrence and defense capabilities, but also for effectively countering the multifaceted impacts of cognitive warfare, which increasingly exploit vulnerabilities in digital networks, information systems, and public perception. Furthermore, this serves as an initial step in a PhD research thesis aimed at offering states solutions for enhancing cyber resilience, with the goal of safeguarding their citizens from the challenges posed by cognitive warfare.

Keywords: Cybersecurity strategies, Cyber resilience, Cognitive warfare, Cognitive dimension, Human factor

1. Introduction

The proliferation of internet access, the expansion of cyberspace, and its integration into daily life have introduced new uncertainties that are not easily addressed within the traditional frameworks of war and conflict. Historically, conflicts and wars between states were conducted within clearly defined territorial contexts. However, in the contemporary era, the arenas of state interaction encompass the human system, the cyber system, and the interplay between the two, rendering the mapping of interactions, methods, and objectives increasingly abstract and complex.

Although the current spectrum of war is different, NATO member states respect Article 5 of the North Atlantic Treaty, which defines an armed attack against one-member state as an attack against all, granting member states the right to legitimate individual or collective defense, including the use of force, to restore and maintain peace. (NATO, 1949) Since the Prague Summit Declaration in 2002, member states have increasingly expressed concerns over cyberattacks, emphasizing the unique challenges posed by the ambiguous nature of the geopolitical landscape in cyberspace. The Alliance's policy on defense and deterrence against adversaries has, in recent years, been framed as a natural response to the evolving landscape of global threats.

We can gain a clear view of the evolving geopolitical landscape by analyzing the 2024 cyber threat trends specific to Romania, as detailed in the Cyber Security Report 2025 by Check Point Research, (CheckPointResearch, 2025) which underscore the evolving tactics of threat actors, the vulnerabilities of state institutions, and the broader cognitive effects on citizens. Notably, disinformation campaigns leveraging artificial intelligence were orchestrated around global events, including the presidential elections, with the intent to destabilize democratic processes and manipulate public opinion. Russian interference played a prominent role, utilizing fake social media accounts, particularly on TikTok, to promote candidate Călin Georgescu. The unexpectedly high percentage of votes garnered by Georgescu in the first round prompted the government to declassify intelligence reports, which revealed extensive foreign interference and led to the annulment of the election results. Additionally, cyberattacks on the healthcare sector emerged as a significant concern, with medical organizations becoming the second most targeted sector. A striking example is the Phobos ransomware attack on Romanian Soft Company, the developer and manager of the Hipocrate information system. (DNSC, 2024) This

attack, executed in a single night, encrypted databases and files across 26 hospitals in Romania, demanding financial compensation for decryption. The subsequent internet disconnection caused severe disruptions, including delayed medical services, slower patient care, and a marked reduction in operational capacity. Although challenging cyber events persist, the impact on population cognition can be mitigated through the implementation and enhancement of cyber resilience strategies.

2. Literature Review on Cyber Resilience

Cyber resilience has gained prominence as traditional security measures have proven insufficient in protecting organizations and populations against evolving cyber threats. A reactive approach to such threats often exacerbates vulnerabilities, prompting the development of advanced systems capable of anticipating, preparing for, adapting to, and rapidly recovering from cyberattacks (Petrenko, 2019). This concept encapsulates the ability to maintain desired outcomes despite challenging events such as cyberattacks, natural disasters, or economic crises. As noted by the National Institute of Standards and Technology (NIST, 2021) resilience is frequently employed as a metaphor to describe how systems respond to external stressors. However, when the metaphor is disentangled from the scientific framework, it becomes evident that the impact of resilience extends beyond system functionality to influence the cognitive responses of individuals. Recognizing this cognitive dimension underscores the need for holistic approaches in cyber resilience strategies, ensuring both technical and psychological readiness in the face of modern threats.

The unrestricted exposure of young people to cyberspace reveals a critical vulnerability in the security chain: the human factor. Ensuring a secure and supportive environment for learning and connection in cyberspace is a shared responsibility, as digital interactions increasingly permeate all aspects of life. The 2022 study *"Why Children Are Unsafe in Cyberspace?"* (Panhans, 2022) serves as a key reference point for identifying the vulnerabilities faced by young people and enhancing cyber resilience in the context of cognitive warfare. This study highlights the risks to individuals aged 8 to 17, including exposure to illegal and age-inappropriate content, embedded gambling, ideological persuasion, exploitation (sexual abuse, trafficking, harassment, drugs), and the misuse of personal data. Further analysis demonstrates that organizational elements and human negligence accounted for 72% of major data breaches reported between 2011 and 2016, with inadequate security technology cited in only 28% of cases (Deutscher, 2018). To echo Graubart, while cyber resilience objectives can be interpreted in various ways, resilience practices are implemented across multiple layers within a layered architecture. This architecture encompasses not only technical measures but also the individuals responsible for carrying out mission functions.(Graubart, 2011) Saleh Mohamed's academic article explores definitions of cyber resilience from 2010 to 2023, critically examining the limitations of redundancy as a sole resilience strategy. It emphasizes the necessity of robust security policies as a foundational measure for effectively addressing widespread cyber threats. (AlHidaifi, 2024) The initial response to the ubiquitous threats faced by younger generations must begin with awareness. Ensuring coordinated action from educators, policymakers, and the private sector is essential for fostering a safer cyberspace, equipping young people with the knowledge and tools to navigate the digital world securely and responsibly.

3. Literature Review on Cognitive Warfare

NATO defines cognitive warfare as "the synchronized use of other instruments of power to influence attitudes and behaviour by affecting, protecting, or disrupting individual and group knowledge to gain an advantage over an adversary" (NATO, NATO's Strategic Warfare Development Command, 2023) . This concept encompasses various dimensions, including challenges to resilience rooted in neuroscience, the exploitation of cognitive biases, the inherent propensity for cognitive errors, the manipulation of perception, attentional saturation or "tunnelling," and the induction of cognitive stress (Claverie, 2021). Cognitive warfare represents the intersection of information warfare (Giles, 2013), psychological operations (PsyOps) (NATO, AJP 3.10.1. , 2007) , and cyber operations, as these approaches collectively aim to compromise physical infrastructures while producing strategic effects in the human domain. While initially conceptualized by NATO as a military strategy, the implications of cognitive warfare extend far beyond the battlefield. Global geopolitics is increasingly shaped by tactics such as coercion, the strategic deployment of political, economic, or financial instruments, and the dissemination of disinformation (Deppe, 2024). These tactics obscure the objectives and intentions of potential adversaries, with their impacts reaching beyond military personnel and assets to influence civilian populations and societal stability.

Cognitive warfare, recognized as the sixth domain of warfare (Kramer, 2023), operates on a battlefield confined to the human body and brain. With rising interconnectivity, its primary objective is to alter perceptions and

behaviours, shaping individual and group beliefs to align with the aggressor's tactical and strategic goals (ESDC, 2023) 4). Technology plays a critical role as a concealed, pervasive, and often undetectable geopolitical weapon, with the impacts on victims being difficult to measure. Cognitive warfare encompasses various methods categorized by their objectives, including network attacks (e.g., network control, antivirus disruption, and deception), psychological operations (propaganda, demoralization, psychological influence, and deception), and the destruction of IT infrastructure (Cheatham, 2024) . Additional tactics, such as cyber data theft and electoral interference, directly target the cognitive domains of individuals, organizations, and societies. As observed, the field of cyber resilience intersects with cognitive science to some extent; however, the specialized literature primarily focuses on psychological aspects. Nonetheless, cognitive effects remain underexplored and are not explicitly developed in existing research. Mitigating these effects requires strengthening societal and cyber resilience, fostering critical thinking, and advancing information literacy, which could be influenced either by the European Union or the North Atlantic Treaty Organization.

4. European Union Approach to Cyber Resilience

The European Union's initiatives in cyber resilience gained momentum in 2020 with the introduction of the new Cybersecurity Strategy by the European Commission. The strategy's first pillar prioritized enhancing cyber resilience across critical sectors, including hospitals, energy networks, railways, public administrations, research laboratories, and medical device manufacturing (EU, 2020), The second pillar emphasized cyber diplomacy, aiming to prevent, deter, and effectively respond to malicious cyber activities, particularly those targeting critical infrastructure, supply chains, institutions, and democratic processes. The third pillar focused on fostering research and innovation in digitalization, with a planned implementation period of seven years under programs such as the Digital Europe Programme (EU, The Digital Europe Programme, 2024) and Horizon Europe (EU, Horizon Europe, 2021). Additionally, the Directive on measures for a high common level of cybersecurity across the Union (EU, The NIS 2 Directive, 2022) expands coverage to medium and large entities across sectors critical to the economy and society.

Complementing the aforementioned frameworks, the European Cyber Resilience Act (CRA) (EU, Cyber Resilience Act, 2024) was introduced in 2024 to strengthen consumer protection. This legislative framework establishes cybersecurity requirements for hardware and software products with digital elements introduced into the European Union market, serving as a critical regulatory tool in an increasingly ambiguous geopolitical landscape. Under the CRA, manufacturers of digital products are required to conduct cybersecurity risk assessments to prevent incidents or mitigate their impact. Additionally, product updates must be provided to users free of charge. User accountability is also emphasized in Annex 1 of the CRA, which mandates transparency regarding manufacturers' identities, including the name, registered trade name, and contact details, enabling users to verify information and reduce the risk of cyberattacks. This approach underscores the EU's commitment to enhancing cyber resilience by addressing the human factor, leveraging institutional mechanisms to safeguard individuals as consumers. However, a legislative gap remains concerning measures to counter the effects of cognitive warfare on the human domain.

The populations of European Union member states benefit from training programs aimed at fostering a measurable understanding of cyber resilience. Specialized insights from Cyber Risk GmbH (GmbH, 2022) shed light on various forms of cyber warfare that target the cognitive domain. Among these, disinformation emerges as a particularly potent tool, designed to destabilize, manipulate, and influence public opinion by leveraging strong emotions such as anger and fear. These emotions, amplified through online messaging, resonate deeply with the psychological vulnerabilities of target audiences. Consequently, the development of cyber resilience must include psychological resilience and critical thinking skills to resist manipulative tactics effectively. Propaganda, as another dimension of cognitive warfare, systematically shapes perceptions, manipulates cognitions, and directs behaviors to achieve the propagandist's objectives. These tactics exploit vulnerabilities across political, military, economic, informational, and social domains. In response, cyber resilience efforts focus on protecting users' personal data across platforms to minimize their exposure to cyberattacks and espionage. A common underlying factor in these phenomena is the "*truth bias*" (Pantazi, 2018), a cognitive tendency linked to how individuals process information. When incoming information aligns with pre-existing beliefs, it reinforces a sense of coherence and stability, even if such alignment distorts perceptions of reality. This cognitive bias underscores the importance of fostering critical awareness to mitigate the impact of disinformation and propaganda on public cognition and resilience.

Promoting cybersecurity awareness through targeted training programs for both manufacturers and consumers is a critical step in mitigating the risks users face in an increasingly complex threat landscape. Furthermore,

enhancing cyber resilience necessitates building coalitions among like-minded nations to support citizens, harmonize national policies, and effectively address risks to data security and privacy. In this context, the European Union continues to play a pivotal role as a key partner for NATO in advancing cyber resilience efforts. Notably, the inaugural Structured Dialogue on Cyber (EEAS, 2024) between the EU and NATO marked a significant milestone, fostering deeper cooperation in cybersecurity and reinforcing collective preparedness in this domain.

5. NATO Approach to Cyber Resilience

In contrast to the European Union's approach to cyber resilience, NATO emphasizes resilience-building as a primarily national responsibility. Despite facing hundreds of cyber incidents monthly (NATO, Cyber defence, 2024), NATO maintains a defensive cyber policy aligned with international obligations. The Alliance's evolving approach to resilience began at the 2021 Brussels Summit and was further articulated in the 2022 Strategic Concept, which emphasized that "*national and collective resilience is an essential basis for deterrence and […] protecting our societies, populations and shared values*" (Shelest, 2021). At the 2023 NATO Summit in Vilnius, member states endorsed enhancing contributions to cyber defense. This included integrating NATO's three levels of cyber defense – political, military, and technical – to ensure effective civil-military cooperation during peace, crisis, and conflict. Additionally, NATO highlighted the importance of engaging with the private sector, where appropriate, to bolster collective cyber resilience.

Beyond annual meetings and unanimous decisions, NATO-led coalition initiatives extend into programs, exercises, and educational efforts aimed at strengthening cyber resilience. A notable example is the NATO Cyber Incident Response Center (NCIRC) in Mons, Belgium (NCIA, 2025), which provides real-time, multi-layered defense and monitoring capabilities. Through the Malware Information Sharing Platform (MISP) (MISP, 2024), NCIRC facilitates the sharing of critical information on diverse cyberattacks, enabling rapid and coordinated responses. Additionally, flagship exercises such as Cyber Coalition (ACT, 2024) and Locked Shields (CCDCOE, 2024) bring together thousands of cyber experts annually. These exercises simulate complex, real-world scenarios, fostering collaboration and enhancing collective security through the development and testing of advanced cyber defense strategies.

NATO's efforts to enhance cyber resilience have been intensifying annually, driven by the increasing complexity and diversity of cyberattacks. However, the approach to cognitive warfare remains limited, with a primary focus on military personnel. In the broader operational context, it falls upon individual states to establish robust legal and practical frameworks to counter the societal impacts of cognitive threats. Of all the NATO member states, in this presentation I will focus on Romania's most significant initiatives and strategies in this domain, highlighting their relevance and effectiveness in addressing cognitive warfare challenges.

6. Romania's Approach on Building Cyber Resilience to Face the Challenges of Cognitive Warfare

Romania's journey in establishing a legal framework for cyber resilience began in 2011 with the creation of the National Cyber Security Incident Response Center (CERT-RO). CERT-RO was initially established as a specialized structure for expertise and research in the protection of cyber infrastructure. A decade later, this structure evolved into the National Cyber Security Directorate (DNSC) through Emergency Ordinance 104/2021, reflecting Romania's commitment to adapting to the growing complexity of cyber threats. Additionally, in 2013, Romania approved the Cyber Security Strategy (RoGov, 2022) and the National Action Plan for implementing the National Cyber Security System. These foundational documents affirmed Romania's role as a coordinator of national cyber security efforts, aligning with EU and NATO strategies. The Strategy emphasizes the resilience of cyber infrastructures as their ability to withstand incidents or attacks and swiftly return to normal functioning. Further enhancing its resilience capabilities, Romania established the Euro-Atlantic Resilience Center (E-ARC) in 2021. (RoGov, National Action Plan on the implementation of the National Cybersecurity System., 2013) This center of excellence partners with NATO and the EU to advance resilience through the development of concepts, doctrines, and methodologies. E-ARC also facilitates knowledge transfer among government entities, the private sector, civil society, and academia. Its mission includes providing specialized training and serving as a platform for collaboration in resilience-related areas. (Ciobotaru, 2024) Together with DNSC, E-ARC underscores Romania's dedication to strengthening national and international cyber resilience in an era marked by escalating cognitive challenges.

Legal frameworks in Romania empower the entire population to address current security incidents by adopting various strategies recommended by specialized agencies and accessing comprehensive resources designed to

mitigate the effects of cyberattacks. One notable example is the "*Adeline"* fraud, which exploited the WhatsApp platform to gain unauthorized access to users' devices. Attackers sent deceptive messages to users' contacts, requesting monetary transfers (DNSC, ALERT: "Vote for Adeline" Fraud, 2025). Another method targets Google Calendar, where attackers send fraudulent invitations that redirect victims to phishing websites, aiming to steal authentication credentials and facilitate financial fraud . (DNSC, Cybersecurity News of the Week (12/19/2024), 2024) The consequences of such cyberattacks extend beyond users' online integrity, affecting their cognitive resilience. Romania has responded by developing practical resources, including the Social Engineering Guide, which explains techniques of persuasion and manipulation employed to exploit victims (DNSC, SOCIAL ENGINEERING, 2024) Similarly, the *Deepfake Guide* offers strategies to counteract media manipulation that replicates voices, actions, or faces to spread misinformation and damage reputations (DNSC, Deepfake - manipulated or informed?, 2024). To further support public awareness, the documentary *How Do I Protect My Personal Data and Defend Myself from Online Dangers?,* produced by the Association of Specialists in Confidentiality and Data Protection, emphasizes achieving a balance between enjoying the online world and maintaining safety. In conclusion, cyber resilience in the face of cognitive challenges relies on a foundation of collaboration, public awareness, personal training, and education, ensuring that all individuals, regardless of age, are equipped to navigate an increasingly complex digital landscape.

7. Tools and Methods to Enhance Cyber Resilience in Response to the Challenges of Cognitive Warfare

At the international level, the European Union (EU), the North Atlantic Treaty Organization (NATO), and Romania have each demonstrated significant progress in developing tools and methods to strengthen cyber resilience in the face of cognitive warfare challenges. At the EU level, the cornerstone document is the Cyber Resilience Act, which establishes cybersecurity requirements aimed at reducing vulnerabilities exploitable in cognitive warfare scenarios. NATO, as the initiator of the cognitive warfare concept, places a strong emphasis on fostering cooperation and sharing lessons learned in the cyber domain among member states, with the overarching goal of maintaining cognitive superiority. Romania, serving as a practical example of a member state active in both organizations, has proactively bolstered its cyber resilience through initiatives that promote collaboration between the public and private sectors. A comparative analysis of these three approaches highlights a series of tools and methods that are particularly relevant for addressing the complexities of cognitive warfare in today's digital age.

Table 1: Tools and methods to enhance cyber resilience in response to the challenges of cognitive warfare

Perspectives	Cyber resilience	Cognitive warfare challenges			
		Disinformation, Propaganda	**Information Manipulation**	**Military intimidation**	**Personal data**
EU	Cyber Resilience Act Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies (CERT-EU)	EU action plan against disinformation Code of Practice on Disinformation	Strategic communication and countering information manipulation ESDC - Foreign Information Manipulation and Interference" (FIMI)	Strategic Compass for Security and Defence (The EU's Rapid Deployment Capacity)	Guidelines 01/2025 on Pseudonymisation GDPR training courses Guidelines on personal data breach notification for the European Union Institutions and Bodies
NATO	NATO Integrated Cyber Defence Centre NATO Cooperative Cyber Defence Centre of Excellence	WMGIC X NATO Countering disinformation challenge	NATO Strategic Communications Centre of Excellence Online course "Introduction to StratCom" Information environment simulation platform "InfoRange"	Cyber exercises: Coalition Warrior Interoperability exercise (CWIX), Trident Juncture, Trident Jaguar, Cyber Coalition) NATO 2022 Strategic Concept	The Rights to Privacy and Data Protection in Armed Conflict

Perspectives	Cyber resilience	Cognitive warfare challenges			
		Disinformation, Propaganda	**Information Manipulation**	**Military intimidation**	**Personal data**
ROMANIA	National cyber security directorate Top Tips to Make Your Home Cyber Safe Practical approaches to building secure applications Euro-Atlantic Center for Resilience	DEEPFAKE - Guide for organizations Mobile malware awareness campaign Tips for remote working NATO Resilience Course for Civil Experts course	SOCIAL engineering Guide for social media account protection and recovery Guide for crisis situations	-	How do I protect my personal data and defend myself from dangers in the online environment? Guide to raising awareness of the importance of personal data protection and cyber security for children, parents, teachers

7.1 Interpretation

Cyber resilience and organizational resilience transcend mere managerial responsibility, relying instead on awareness, involvement, and adaptability across all levels of an organization. Effective and efficient communication, both horizontally and vertically, forms the foundation for achieving sustainable and impactful results. The European Union exemplifies a proactive stance in safeguarding citizens, not only by regulating digital products introduced to its market but also by facilitating specialized training in cyber resilience. However, mitigating the effects of cognitive warfare depends fundamentally on fostering awareness and disseminating accurate information. NATO complements this approach by emphasizing practical tools, including cyber exercises, international cooperation, and strategic communication. As reiterated in its 2022 Strategic Concept, NATO underscores its commitment to protecting both military and civilian sectors, highlighting the critical importance of resilience in the face of evolving threats. Romania, for its part, stands as a model of responsibility, proactively safeguarding its population by emphasizing the significance of security incident reporting, responsive measures, awareness initiatives, and the anticipation of cyber events that could compromise the physical and psychological integrity of its citizens.

Collectively, these efforts present a diverse spectrum of tools and methods to cultivate robust cyber resilience. However, at the heart of cyber warfare lies the human factor—the ultimate epicentre. It is essential for individuals to develop the ability to discern credible information from assertions and remain vigilant against the vulnerabilities posed by pre-existing beliefs and relationships. By prioritizing the human element, nations and organizations can better navigate the challenges of cognitive and cyber warfare.

At the international level, cyber resilience training programs provided by EU and Romania serve as essential tools for individuals, whether they act as cyber consumers or cyber producers. These programs incorporate a diverse range of specialized methodologies, spanning from information systems security, risk management, and coding theory to data storage security. Additionally, they include targeted training such as Information Security Awareness, Social Engineering Awareness and Defense, and sector-specific courses like *The Target is the Bank: From Hacking to Cybercrime and Cyber Espionage*. (GmbH, 2024) These initiatives play a crucial role in strengthening global cyber resilience by equipping individuals with the necessary skills to navigate and counter evolving cyber threats. Another effective approach to raising awareness of the risks associated with internet access involves the use of continuously updated practical guides, alongside the identification and public reporting of cyberattacks. Providing tangible solutions and encouraging incident reporting not only enhances cybersecurity preparedness but also fosters a sense of collective resilience. By recognizing that cyber threats impact many individuals and organizations, these initiatives help mitigate fear, promote knowledge-sharing, and empower people to respond more effectively to cyber incidents.

8. Conclusions

The rapidly evolving landscape of cognitive warfare and cyber threats underscores the critical need for adaptive and multifaceted strategies to build resilience at individual, organizational, and societal levels. Efforts such as enhancing digital literacy across generations, fostering critical thinking, and raising awareness through targeted campaigns are foundational to equipping societies to discern and counteract disinformation. Moreover, leveraging technology responsibly, promoting positive mobilization via social media, and implementing robust

cybersecurity practices collectively contribute to creating a stronger defense against manipulation and exploitation in the digital space.

The role of collaboration between public and private sectors is increasingly pivotal in shaping the informational environment. Private corporations, as key players in the digital ecosystem, must align their practices with democratic values and ethical standards, working in tandem with policymakers to ensure secure and trustworthy information systems. Initiatives such as NATO's cybersecurity strategies, EU regulations, and Romania's educational and policy measures highlight the importance of integrated and strategic approaches to cyber resilience. These efforts, coupled with the proactive engagement of citizens and institutions, serve as a bulwark against emerging cognitive and cyber threats.

Ultimately, human-cantered strategies remain at the heart of effective resilience-building. Recognizing the emotional and cognitive dimensions of manipulation, prioritizing community awareness, and fostering cognitive agility are essential for addressing the non-kinetic threats of the modern era. Based on the findings of the study, it is evident that cognitive warfare cannot be fought solely by an army; it is, at its core, a deeply personal battle. Its success depends not only on the support of state institutions but also on the cognition and awareness of each individual, which hold the power to either prevent conflict or sustain it.

In conclusion, by integrating insights from NATO, the EU, and Romania, we can develop a multi-layered cyber resilience framework that safeguards human cognition against psychological manipulation. However, the extent to which states can effectively support public awareness and precautionary measures regarding online activity remains a subject of ongoing debate. These concerns will be further explored in my broader PhD research study, which will examine the role of strategic ambiguity and the geopolitics of metaphor in the 21st century, shedding light on their implications for cognitive security and cyber resilience.

References

ACT. (2024). *Cyber Coalition: NATO's Flagship Cyber Exercise*. Retrieved from Allied Command Transformation: https://www.act.nato.int/activities/cyber-coalition/

AlHidaifi, S. M. (2024). A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions. *ACM Digital Lybrary*, 7.

CCDCOE. (2024). *Locked Shields 2024 Sets the Stage for Advancing Global Cyber Defence*. Retrieved from NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/news/2024/locked-shields-2024-sets-the-stage-for-advancing-global-cyber-defence/

Cheatham, M. J. (2024). Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone. *National Defence University*.

CheckPointResearch. (2025). *The State of Cyber Security 2025, top threats, emerging trends, and CISO recommandations. .* Check Point SoftwareTechnologies.

Ciobotaru, M.-E. (2024). *Digital resilience tools. Decision-making amid information overload.* Retrieved from Euro-Atlantic Resilience Centre: https://e-arc.ro/2024/09/16/digital-resilience-tools-decision-making-amid-information-overload/

Claverie, B. (2021). *Des théories pour la cognition. .* L`Harmattan.

Deppe, C. (2024). *Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. .* Frontiers, 4.

Deutscher, S. A. (2018). *How to build a Cyber Resilient Organization. .* CRC Press.

DNSC. (2024). Alert: Backmydata Ransomware. *National Cyber Security Directorate*.

DNSC. (2024, December 19). *Cybersecurity News of the Week (12/19/2024)*. Retrieved from National Cybersecurity Directorate: https://dnsc.ro/citeste/stirile-saptamanii-din-cybersecurity-19-12-2024

DNSC. (2024). *Deepfake - manipulated or informed?* Bucharest: National Cyber Security Directorate.

DNSC. (2024). *SOCIAL ENGINEERING.* Bucharest: National Cyber Security Directorate.

DNSC. (2025, January 15). *ALERT: "Vote for Adeline" Fraud*. Retrieved from National Cyber Security Directorate: https://dnsc.ro/citeste/alerta-frauda-de-tip-voteaza-pe-adeline

EEAS. (2024, October 04). *European Union and NATO hold the first Structured Dialogue on Cyber*. Retrieved from The diplomatic service of the European Union: https://www.eeas.europa.eu/eeas/european-union-and-nato-hold-first-structured-dialogue-cyber-0_en

ESDC. (2023). *Cognitive warfare in the new international competition: an emerging challenge for the EU PILOT Course*. Retrieved from European Security and Defence College: https://esdc.europa.eu/2024/05/28/cognitive-warfare-in-the-new-international-competition-an-emerging-challenge-for-the-eu-pilot-course/#:~:text=%E2%80%9CIn%20cognitive%20warfare%2C%20the%20human,aggressor's%20tactical%20and%20strategic%20objectives.

EU. (2020). New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. *European Commission*.

EU. (2021). Horizon Europe. *European Commission*.

EU. (2022). The NIS 2 Directive.

EU. (2024). Cyber Resilience Act. *European Commission*.

EU. (2024). The Digital Europe Programme. *European Commission*.
Giles, K. (2013). Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. *NATO CCD COE Publications, 7.*
GmbH. (2024). *The target is the bank: From cybercrime to cyberespionage*. Retrieved from Cyber Risk GmbH: https://www.cyber-risk-gmbh.com/5_The_Target_Is_The_Bank.html
GmbH, C. R. (2022). Cyber Risk GmbH . *European Commission*.
Graubart, D. J. (2011). *Cyber Resiliency Engineering Framework.* MITRE.
Kramer, F. D. (2023). The sixth domain: The role of the private sector in warfare. *Atlantic Council*.
MISP. (2024). *Features of MISP, the open source threat sharing platform.* Retrieved from MISP Threat Sharing: https://www.misp-project.org/features/
NATO. (1949). *The North Atlantic Treaty.* North Atlantic Treaty Organisation.
NATO. (2007). *AJP 3.10.1. North Atlantic Treaty Organization.* NATO ALLIED JOINT DOCTRINE FOR PSYCHOLOGICA LOPERATIONS.
NATO. (2023). *NATO's Strategic Warfare Development Command*. Retrieved from ALLIED COMMAND TRANSFORMATION:: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/
NATO. (2024, July 30). *Cyber defence*. Retrieved from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/topics_78170.htm
NCIA. (2025). *Cyber Defence*. Retrieved from NATO Communications and Information Agency: https://www.ncia.nato.int/about-us/cyber-defence
NIST. (2021). *Glossary. NIST Special Publication 800-160, Volume 2.* National Institute of Standars and Technology.
Panhans, D. (2022). Why Children are unsafe in Cyberspace? . *Global Cybersecurity Forum.*
Pantazi, M. (2018). *The power of the Truth Bias: false information affects memory and judgment even in the absence of distraction. .* Guilford Press Periodicals, .
Petrenko, S. (2019). *Cyber Resilience. .* Gistrup Denmark: River Publishers.
RoGov. (2013). *Cybersecurity Strategy of Romania and the National Action Plan on the implementation of the National Cybersecurity System.* Retrieved from Government of Romania: https://lege5.ro/
RoGov. (2022). *Romania's Cybersecurity Strategy for the period 2022-2027.* Retrieved from Government of Romania: https://lege5.ro/Gratuit/geydinrtga2dq/hotararea-nr-1321-2021-privind-aprobarea-strategiei-de-securitate-cibernetica-a-romaniei-pentru-perioada-2022-2027-precum-si-a-planului-de-actiune-pentru-implementarea-strategiei-de-securitate-ciberne#:~:text=Hot%C4%
Shelest, H. (2021). *NATO"s resilience concept and Ukraine.* NATO.