A National Security Perspective on Strengthening E.U. Civilian-Defence Cybersecurity Synergy: A Systemic Approach

Niculae IANCU
Constanta Maritime University; West University of Timisoara, Romania
nicu.iancu@marcyscoe.org, Niculae.iancu@e-uvt.ro

Abstract

The integration of civilian and defence sectors within the European Union's cybersecurity framework has become a strategic priority, driven by the increasingly complex nature of digital threats to both national and collective security. This paper examines the need for a systematic approach to enhance civilian-defence cybersecurity synergy, emphasising the importance of coordinated efforts to address a range of challenges, including ransomware, state-sponsored attacks, and hybrid warfare. The study highlights the strategic importance of this integration for national and E.U.-wide interests, identifying key obstacles such as fragmented policy frameworks, operational cultural differences, and resource allocation disparities. To bridge these gaps, the paper proposes strategic solutions, including regulatory harmonisation, joint training programmes, and investment in dual-use technologies. The research underscores the critical role of a unified policy approach in facilitating efficient resource allocation, streamlined communication, and faster incident response. Additionally, it explores the potential of emerging technologies, such as AI and quantum computing, to strengthen cybersecurity capabilities across sectors. Ultimately, the integration of civilian and defence efforts within the E.U.'s cybersecurity ecosystem is essential for building a resilient, cohesive, and adaptive framework, ensuring the protection of digital infrastructure, enhancing national security, and reinforcing the E.U.'s global leadership in cybersecurity.

Index terms: cybersecurity civilian-defence integration, E.U. cybersecurity framework, cyber threats, national security, E.U. sovereignty in cyberspace

1. Introduction

In this era defined by rapid technological advancements and increasing digitalisation, the European Union faces a growing array of cyber threats that pose significant risks to both national and collective security. Cyber incidents have evolved in complexity and scope, ranging from ransomware attacks and data breaches to sophisticated state-sponsored operations and hybrid warfare tactics. These threats can disrupt critical infrastructures, undermine public trust, and weaken the resilience of national economies. The integration of digital systems across civilian sectors—such as finance, healthcare, energy, and transportation—has made these infrastructures particularly vulnerable, heightening the urgency for a robust and coordinated cybersecurity strategy.

Traditionally, the responsibility for national security, including the defence against external threats, has been vested in the defence sector. However, the nature of cyber threats transcends traditional boundaries, often targeting civilian infrastructures and leveraging vulnerabilities in interconnected digital networks. This convergence of civilian and national security concerns necessitates a new approach that integrates the strengths of both sectors. The E.U. has recognised this

need, prompting efforts to enhance synergy between civilian and defence entities within its cybersecurity framework. Effective collaboration between these sectors is critical to developing a coordinated response capable of addressing both conventional and emerging threats, ensuring the security and resilience of national and collective E.U. interests.

Despite the strategic importance of this integration, several challenges hinder the development of a cohesive cybersecurity ecosystem across the E.U. Fragmented and ambiguous policy frameworks, differences in operational cultures, and disparities in resource allocation are among the key obstacles that need to be addressed. The lack of harmonised regulations and inconsistent information-sharing protocols can create gaps in defence measures, making it easier for adversaries to exploit vulnerabilities. Additionally, the civilian sector often faces budget constraints that limit the adoption of advanced cybersecurity technologies, while the defence sector, although well-resourced, may lack the flexibility and innovation-driven approach that characterises civilian tech industries.

This paper explores a systematic approach to strengthening the synergy between civilian and defence sectors within the E.U.'s cybersecurity framework. It examines the strategic importance of this integration, identifies key challenges, and proposes solutions to bridge existing gaps. By focusing on regulatory harmonisation, joint training programmes, and investment in dual-use technologies, this study aims to highlight effective strategies for building a cohesive and resilient cybersecurity ecosystem. Additionally, the paper discusses the potential of emerging technologies, such as artificial intelligence (AI) and quantum computing, to enhance cybersecurity capabilities across sectors. Ultimately, this research advocates for a unified policy approach that facilitates efficient resource allocation, streamlined communication, and faster incident response, reinforcing the E.U.'s position as a global leader in cybersecurity while ensuring the protection of its digital infrastructure and national security.

2. Rising Importance of Cybersecurity in National Security

In the contemporary security landscape, the increasing reliance on digital technologies across all sectors of society has dramatically elevated the significance of cybersecurity as a core element of national security. Traditionally, national security was defined through the lens of military strength, state sovereignty, and territorial integrity [1]-[3]. The post-Cold War era expanded the traditional approach to security by introducing non-military dimensions such as economic, societal, and environmental concerns [4]. More recently, the digital revolution has further extended the scope of what constitutes a security threat, incorporating new dimensions that transcend physical borders and include cyberattacks on critical infrastructure, cybercrime, cyber espionage, and the disruption of political processes using digital tools [5].

Cybersecurity has become an essential pillar of national security as states and non-state actors recognise the potential of cyberattacks to cause widespread disruption and damage to a nation’s critical infrastructure, as well as its citizens and society as a whole. The vulnerabilities in sectors such as finance, healthcare, energy, and telecommunications make them prime targets for cyberattacks, which can wipeout essential services and erode public trust. The cyber domain has introduced a new form of power—cyber power—which encompasses both the capacity to defend critical digital assets and the ability to disrupt adversaries' systems [6]. This shift has necessitated a redefinition of what constitutes a national security threat, elevating cyber threats to the top of the security agenda and placing cybersecurity at the centre of state defence mechanisms.

For example, in line with global trends, since 2016, Romania’s National Security Strategies have encapsulated the growing prominence of cybersecurity as a national security priority. In its 2010 edition, Romanian policymakers moved ‘beyond regional instability and terrorism’ to also examine ‘new risks and threats, such as pandemics, natural disasters, and cyber or energy security’. Although at the time they assumed that ‘such threats do not directly affect the state’, they recognised that many

of these new factors, 'radicalised as a result of the current evolution of globalisation, can seriously affect the quality of life and call into question the citizen's safety' [7]. The 2015 National Security Strategy addressed cyber issues in its security threats assessment, highlighting the growing concern of 'cyber threats initiated by hostile entities, both state and non-state'. These threats target 'informational infrastructures of strategic interest to public institutions and companies'. The strategy specifically highlighted the threat of 'cyberattacks carried out by cybercrime groups or extremist hackers, which directly undermine Romania's national security,' advancing the cyber domain to a major national security concern. This focus on cybersecurity marks a notable evolution compared with previous National Security Strategies, demonstrating an increased recognition of the critical and expanding nature of cyber threats to national security.

The current 2020 National Security Strategy further develops the concept of cybersecurity by unequivocally integrating it into the 'extended national security concept', positioning it on the same level with traditional security domains such as 'defence, foreign policy, public order, intelligence, counterintelligence, and security'. [8] This demonstrates a 'multi-dimensional approach to security' [8], tailored to meet the increasingly complex security challenges of the modern world, while also reflecting Romania's alignment with Euro-Atlantic strategic thinking. Such a vision ensures the 'resilience' of vital sectors, including energy, finance, and critical infrastructure [8], reflecting a broader understanding that cybersecurity is now an integral component of national defence systems which can no longer be neglected or underfunded.

The militarisation of cyberspace further underscores the growing importance of cybersecurity in national and alliance settings. States have increasingly recognised cyberspace as the fifth domain of warfare, alongside land, sea, air, and space. This strategic shift is reflected in the strategies and doctrines of national governments and international security organisations, which now include dedicated cyber defence units within their military and intelligence agencies. For instance, NATO officially recognised cyberspace as a domain of operations in 2016, indicating the strategic importance of securing digital infrastructure to maintain national and international security [9]. Similarly, several 'great power competitors' [10], including the United States, China, and Russia, have established cyber commands responsible for both defensive and offensive cyber operations [11]. The pursuit of strategic advantage and dominance now extends well beyond conventional warfare, with cyberspace emerging as a critical arena for geopolitical competition. This has led these and many other nations to invest heavily in developing advanced cyber capabilities, both for executing cyberattacks and for defending against potential threats, thereby establishing cyberspace as a critical domain of future warfare [12]. This demonstrates a growing recognition that cyber threats have the potential to cause significant harm comparable to traditional military attacks, if not greater, because of the interconnectedness of global systems.

One of the most critical developments in the global nexus between cybersecurity and national security is the concept of hybrid warfare [13]. Hybrid warfare combines conventional military tactics with irregular tactics, such as cyberattacks, disinformation campaigns, and economic coercion, to destabilise adversaries [14]. The cyber dimension of hybrid warfare allows adversaries to conduct asymmetric operations that are difficult to trace and even harder to attribute. This is particularly concerning for national security and allied defence because it complicates the conventional understanding of conflict, making it more difficult for states to respond effectively to these threats.

For example, Russia's cyber operations against Ukraine in 2014, which accompanied its annexation of Crimea, are a prime example of hybrid warfare. These operations included targeted attacks on Ukraine's critical infrastructure, including energy grids, and extensive disinformation campaigns to destabilise the political environment [15]. Since the full-scale Russian invasion of Ukraine in 2022, cyber warfare has complemented the conventional forces engaged in conflict, further demonstrating how cyberattacks have been integrated into broader military strategies. Cyberattacks were used not only to undermine state functions and disturb adversary military

technologies but also to erode public confidence and create confusion, thereby weakening the state's ability to respond to more traditional military threats. This demonstrates the intricate role cybersecurity now plays in the broader national security calculus, especially in the context of hybrid threats.

Moreover, non-state actors have also recognised the potential of cyberattacks to influence national security. Terrorist organisations have attempted to develop cyber capabilities that could be used to disrupt government functions or critical infrastructure, though their success has been limited thus far [16]. However, the increasing availability of cyber tools on the black market and the proliferation of sophisticated hacking techniques raise concerns about the future capabilities of such groups. Cyber warfare, therefore, poses a multilayered threat, not just from state actors but from a diverse array of non-state actors who could leverage these tools to undermine national security.

The rapid advancement of technology, particularly in fields like artificial intelligence (AI), the Internet of Things (IoT), and quantum computing, is reshaping the nature of cybersecurity challenges. As these technologies become more integrated into the fabric of society, they create new vulnerabilities that can be exploited by cyber adversaries. For example, the proliferation of IoT devices in critical infrastructure has expanded the attack surface for cyberattacks, making it easier for malicious actors to gain access to sensitive systems, including those vital to national security [17].

Especially, AI poses a significant dual-use dilemma in cybersecurity. On one hand, it offers the potential to enhance defensive capabilities by improving threat detection and automating responses to cyber incidents [18]. AI-driven systems analyse network traffic and user behaviour, identifying anomalies that may indicate a breach. These systems can autonomously respond by isolating compromised systems, preventing further damage, and acting as autonomous response tools without requiring human intervention [19]. In the defence sector, AI has been applied to detect malware more effectively by analysing large datasets and recognising patterns indicative of cyber threats. NATO, for example, has made significant investments in AI-powered cybersecurity systems, enabling them to predict and block cyber intrusions pre-emptively, especially in the face of zero-day attacks that exploit previously unknown vulnerabilities [20].

However, while AI has enhanced cybersecurity defences, it has also been weaponised by adversaries to launch more sophisticated attacks that evade traditional defence mechanisms [18]. AI-powered malware hides malicious code within legitimate applications and only triggers when certain conditions, such as facial recognition, are met. This targeted and highly evasive nature makes it difficult to detect using conventional defences, posing a significant challenge for cybersecurity professionals [21]. Moreover, AI is increasingly being utilised by cybercriminals to orchestrate more sophisticated phishing attacks. By analysing data from social media, emails, and other online activities, AI can generate highly personalised phishing messages that are much harder to distinguish from legitimate communication.

In addition to these AI threats, the emergence of quantum computing presents another significant challenge to cybersecurity. Quantum computing promises to exponentially increase computational power, potentially rendering current cryptographic systems obsolete. While still in its developmental stages, the race to achieve quantum supremacy is raising concerns about the future security of data and communications. Many nations are now investing heavily in quantum-resistant cryptography to mitigate these risks, recognising that cybersecurity will become even more crucial as we enter the quantum era [22].

The dual-use nature of emerging technologies complicates efforts to secure national digital infrastructures. As adversaries continue to adapt and exploit these new capabilities, both civilian and military sectors must remain vigilant and invest in advanced defence technologies to stay ahead in the cybersecurity arms race.

Consequently, the rising importance of cybersecurity within national security frameworks reflects broader trends in global politics and technology. As the digitalisation of critical infrastructure

and state functions continues, the cyber domain will increasingly define the contours of national security threats. State and non-state actors alike are capitalising on the vulnerabilities inherent in digital systems, and the militarisation of cyberspace further heightens the urgency of establishing robust cybersecurity measures.

Ultimately, cybersecurity is no longer a peripheral concern; it is central to the protection of national sovereignty, the integrity of critical infrastructure, and the stability of political systems. Governments must, therefore, prioritise the development of integrated cybersecurity strategies that involve, at their core, international cooperation, to navigate the complex threat landscape of the 21st century. The increasing importance of cybersecurity within national security frameworks has not only reshaped national strategies, as seen in Romania's evolving approach, but has also demanded greater coordination at the supranational level. The European Union, recognising the interconnectedness of digital infrastructure and the complexity of modern cyber threats, has taken steps to harmonise civilian and defence cybersecurity efforts across member states. As cyber threats grow in scope and sophistication, the need for an integrated approach that leverages both civilian and defence capabilities becomes ever more pressing.

3. The E.U.'s Strategic Imperative for Cyber Resilience and Sovereignty

The European Union has emerged as a global leader in developing comprehensive cybersecurity frameworks, recognising the increasing complexity and scale of digital threats in the modern era. At the core of the E.U.'s cybersecurity policy lies the strategic imperative to safeguard critical infrastructures and ensure the stability of its interconnected digital economies. This policy framework not only seeks to defend against cyber threats posed by both state and non-state actors but also actively fosters technological innovation and leadership within the digital domain, thereby enhancing the E.U.’s global competitiveness. By promoting resilience across member states, the E.U. aims to mitigate vulnerabilities that adversaries might exploit. Furthermore, the framework is forward-looking, focusing not only on defensive measures but also on cultivating innovation, which is vital for maintaining leadership in the digital sphere and ensuring stability and security in the rapidly evolving cyber landscape.

The complexity of modern cyber threats, which includes espionage, ransomware, and hybrid warfare tactics, necessitates a coordinated response across member states. Promoting stability through cybersecurity measures is essential for safeguarding critical services like transport, energy, health, and finance, all of which are highly interconnected and increasingly dependent on network and information systems. As the number of connected devices is expected to grow exponentially, with a significant portion located in Europe, vulnerabilities to cyberattacks are set to increase dramatically in the near future [23].

Defending against a broad spectrum of cyber threats is vital for the E.U. Cyberattacks have the potential to destabilise economies, disrupt governance, and erode public trust. The malicious targeting of critical infrastructure, such as energy grids and communication networks, represents a major global risk. The internet’s decentralised nature, which has allowed it to support exponential increases in traffic, has also left it vulnerable to geopolitical tensions. These tensions, combined with the concentration of essential internet services in the hands of a few private companies, expose the European economy and society to disruptive events that could impact millions. In 2023, approximately 70% of the incidents responded to by cybersecurity teams involved critical infrastructure sectors [24]. This marks a sharp increase in both the scale and frequency of attacks compared to previous years, likely exacerbated by the ongoing geopolitical tensions and digital transformation efforts across Europe.

In this intricate security context, the E.U.’s cybersecurity strategy has been shaped by the increasing frequency of cyberattacks on critical sectors and growing geopolitical tensions, which have

emphasised the urgent need for a robust and coordinated cybersecurity policy across the Union. The European Commission has recognised that cyber threats transcend national borders, making cooperation among member states essential for safeguarding interconnected digital infrastructures [23]. To address these threats, the E.U. has developed a comprehensive cybersecurity strategy that integrates both civilian and defence sectors, but without clearly delineating their roles. This lack of distinction introduces significant challenges, particularly concerning governance, resource allocation, and the differing priorities of each sector. The absence of clear boundaries raises critical questions about coordination, especially regarding the prevention of overlaps in technology development and the avoidance of operational redundancies. These challenges must be managed effectively to ensure that both sectors function efficiently and complement each other in addressing modern cyber threats.

Fostering innovation in cybersecurity is also critical to maintaining the EU's competitiveness. Cybersecurity innovation, driven by cross-border collaboration and investment in research and development, ensures that Europe remains resilient in the face of emerging threats. However, the increasing sophistication of cyberattacks, often combining disinformation campaigns with infrastructure attacks, highlights the need for stronger EU-wide cybersecurity mechanisms.

The shortage of cybersecurity skills within the EU presents another major challenge. Despite the critical nature of cybersecurity, around 291,000 posts for cybersecurity professionals remained unfilled across Europe in 2022, leaving organisations vulnerable to attacks. Additionally, over two-thirds of European companies, particularly SMEs, are considered 'novices' in cybersecurity preparedness, compared to their counterparts in Asia and America. The impact of these shortcomings is significant, with cybersecurity incidents often triggering chain reactions that affect the wider economy and society. Trust in digital tools and services is paramount, and concerns over security continue to deter many Europeans from fully engaging with online services. Reports indicate that nearly two-fifths of EU citizens have experienced security-related problems, and three-fifths feel unequipped to protect themselves against cybercrime [25].

Improving cybersecurity is essential for building trust in digital services, safeguarding privacy, and ensuring the security of personal data. It also underpins the digital transformation of Europe's economy and society, driving benefits such as more flexible workplaces, smarter transport systems, and cleaner energy grids. The EU's new Cybersecurity Strategy for the Digital Decade addresses these concerns and lays out a framework for protecting its people, businesses, and institutions from cyber threats. By fostering a secure and open cyberspace, the EU aims to enhance international cooperation, protect democratic values, and ensure the long-term stability and prosperity of its member states [23].

Moreover, a central objective of the overarching E.U.'s cybersecurity policy is the attainment of digital sovereignty. This concept refers to the E.U.'s capacity to assert control over and safeguard its digital infrastructure, minimising reliance on external actors. By doing so, the E.U. seeks to demonstrate its 'leadership and strategic autonomy in the digital domain'. [36]. Achieving digital sovereignty not only enhances the Union's resilience to external threats but also positions it as a global leader in shaping the future of cybersecurity and technological governance, ensuring that critical infrastructures and data remain under European control. This is crucial for securing critical technologies, data, and infrastructures from third-party interference. Cybersecurity is fundamental in this regard, as it enables the E.U. to safeguard its digital assets while promoting the development of indigenous technological capabilities [26].

The Cybersecurity Act of 2019 is a pivotal step towards achieving digital sovereignty. While strengthening the role of the E.U. Agency for Cybersecurity (ENISA), the Act established a cybersecurity certification framework for ICT products and services, ensuring high standards of security across the Union. This certification framework plays a vital role in ensuring that E.U. member states and businesses adhere to uniform cybersecurity protocols, thus reducing the risk of cyberattacks on critical infrastructures [27].

4. Bridging the Cyber Divide by Integrating Civilian and Defence Sectors in the EU Cybersecurity Strategy

In the European Union's cybersecurity landscape, the roles of the civilian and defence sectors are distinct yet highly complementary, ensuring a comprehensive approach to tackling both civilian and national security cyber threats. The civilian sector, composed of private companies, public institutions, and critical infrastructure operators, is largely responsible for securing economic and public service infrastructures. Their focus is on ensuring resilience, business continuity, and safeguarding consumer data and privacy. This includes protection against common cyber threats like ransomware, phishing, and data breaches, which are often directed at large businesses and public services, such as hospitals, energy grids, and financial systems. Civilian cybersecurity efforts are typically centred around passive defences, such as firewalls, encryption, and regular vulnerability assessments, aimed at mitigating risks and improving incident response capabilities [27][28].

On the other hand, the defence sector is tasked with protecting national and collective security interests, often involving more advanced and proactive cyber defence measures. This sector not only focuses on defending military infrastructures but also conducts intelligence operations, counters cyber espionage from state actors, and employs offensive cyber capabilities when necessary. As hybrid threats, such as disinformation campaigns and attacks on critical infrastructure, become more prevalent, military cyber defence teams must stay ahead of emerging threats by leveraging cutting-edge technologies like AI and quantum cryptography [23].

Despite the distinct roles of the civilian and defence sectors, there is a growing recognition that synergies between the two are essential for creating a comprehensive cybersecurity framework in the E.U. Threats to critical infrastructure, for instance, have both civilian and national security implications, which require joint efforts for incident response and resilience planning. However, defence remains primarily a national responsibility, closely tied to national sovereignty. This contrasts with the broader vision of a European Defence Union, first championed by the E.U.'s founding figures, remarkably Jean Monnet and Robert Schuman. While their early aspirations included integrating defence policies as part of a politically unified Europe - illustrated by the European Defence Community proposal in 1952 - such a union has yet to fully materialise. Defence continues to be governed predominantly at the national level, with initiatives under the Common Security and Defence Policy (CSDP) representing incremental steps toward, but not fully realising, the collective defence envisioned by these early architects of European unity.

This tension between national sovereignty and collective defence has structurally influenced the relationship between the defence and civilian sectors in the E.U.'s cybersecurity efforts. While the defence sector prioritises the protection of classified information and operates within a framework of secrecy, civilian agencies focus on transparency and broad information-sharing, driven by economic and ethical considerations. These differing approaches present challenges to fostering effective cooperation. Bridging these differences is crucial to developing a more integrated cybersecurity strategy, one that can leverage the strengths of both sectors while addressing the growing complexities of modern cyber threats.

As E.U. policymakers envision a more integrated and resilient security framework, particularly with the guidance of the 2022 E.U. Strategic Compass, which acts as a de facto E.U. Grand Strategy, the need for enhanced cooperation between civilian and defence sectors becomes increasingly vital. The Strategic Compass emphasises the growing necessity to protect the E.U.'s most critical processes, assets, and information, particularly as its institutions are subject to an increasing number of cyberattacks and system intrusion attempts. Strengthening the intelligence picture, ensuring trustworthy communication systems, and streamlining security rules across the Union are central to this vision [29].

A common approach by Member States, E.U. institutions, bodies, and agencies, including CSDP missions and operations, is required to protect information, infrastructure, and communication systems. This will necessitate significant investments in state-of-the-art European technical equipment, infrastructure, and expertise. Building on the E.U. Cybersecurity Strategy, the Strategic Compass calls for the adoption of additional standards and rules on information and cyber security, as well as the protection of both classified and sensitive non-classified information within E.U. institutions. [29] These efforts aim to facilitate more secure exchanges between Member States, while bolstering the common approach to cybersecurity across the Union.

Particularly, the Digital Europe Programme, launched in 2021, aims to strengthen the E.U.'s digital capacities by investing in cybersecurity, artificial intelligence, and high-performance computing. This programme fosters synergy between the civilian and defence sectors by encouraging collaboration on research, development, and innovation in cybersecurity technologies [28]. Notably, it marks the first time in E.U. history that the European Commission has utilised a common budget to finance civil-defence synergy in cybersecurity. For example, the 'Strengthening Synergies in Defence and Civilian Cybersecurity-ECYBRIDGE' project is an ambitious initiative of 17 organisations funded by the E.U. to unify the cybersecurity capabilities of civilian and defence sectors across the E.U. [30].

To build on these synergies, it is essential to extend collaborative efforts to other E.U.-funded programmes such as the Permanent Structured Cooperation (PESCO), the European Defence Fund (EDF), and Horizon Europe. Each of these initiatives offers unique opportunities to strengthen the integration between the civilian and defence sectors. PESCO, for instance, encourages deeper defence cooperation among E.U. member states, facilitating joint projects and the development of shared capabilities. By aligning PESCO projects with cybersecurity initiatives, the E.U. can enhance its collective defence posture while addressing cyber threats that may compromise military operations and infrastructures [31]. Similarly, EDF focuses on fostering innovation and collaboration in defence research and development. By integrating cybersecurity advancements into EDF projects, the E.U. can ensure that both civilian and military domains benefit from cutting-edge technologies, reinforcing overall cyber resilience [32].

Additionally, Horizon Europe, the E.U.'s flagship research and innovation programme, supports the development of new technologies and solutions across multiple sectors. Leveraging Horizon Europe's resources for cybersecurity research can drive innovation and the creation of robust cybersecurity tools, enabling the civilian and defence sectors to adapt to evolving threats [33].

By strategically combining the strengths of these programmes, the E.U. can create a more cohesive and comprehensive approach to cybersecurity, ensuring that its digital infrastructure, economic interests, and national security are well protected against a wide range of cyber threats.

5. A Systematic Approach for Strengthening Civilian-Defence Cybersecurity Synergy

A systematic approach to strengthening the synergy between civilian and defence sectors within the E.U.'s cybersecurity framework has become a strategic necessity in the face of evolving digital threats. For member states, this integration is critical to address the complex and multifaceted nature of modern cyber threats, ranging from ransomware and data breaches to state-sponsored attacks and hybrid warfare tactics. Effective collaboration between civilian and defence entities is essential for a robust, coordinated response capable of addressing both conventional and emerging threats, ensuring the security and resilience of national and collective E.U. interests.

The rationale for greater integration is rooted in the interconnected nature of modern society's digital infrastructure, where disruptions can have cascading effects across vital sectors. Civilian entities, such as private companies and critical infrastructure operators, typically act as the first line of defence against these threats. However, their efforts could be significantly enhanced by the

technological capabilities, strategic intelligence, and resources that defence sectors bring to the table. Research has shown that such integration leads to more cohesive and adaptable defences, reducing the chances of system vulnerabilities being exploited by adversaries.

Traditionally, the defence sector has borne the responsibility of safeguarding national security, focusing on preventing hostile actions against the state, including cyber espionage and cyberattacks from state actors. In contrast, civilian agencies have concentrated on protecting data privacy, ensuring business continuity, and maintaining public trust. However, the lines between these domains have blurred significantly, as evidenced by incidents where state-sponsored attacks have targeted civilian infrastructure, creating widespread disruption and undermining public confidence [34]. This convergence underscores the need for a comprehensive approach that integrates the strengths of both sectors, fortifying the E.U.'s overall cybersecurity posture.

One of the primary obstacles to achieving effective integration between the civilian and defence sectors is the difference in operational cultures. The defence sector traditionally operates under strict protocols of secrecy, which often restricts information-sharing and can hinder collaboration with civilian entities that prioritise open communication and cooperation. Additionally, the regulatory and legal frameworks governing the civilian and defence sectors vary significantly, complicating efforts to establish cohesive guidelines for technological and operational cooperation without compromising national security imperatives. Creating a regulatory environment that fosters cooperation between these sectors requires nuanced policy development that acknowledges their distinct yet complementary roles.

From a political perspective within the E.U., coordinated policy efforts are essential to bridge these divides. Member states must work towards creating a regulatory framework that facilitates cooperation between civilian and defence sectors while respecting their distinct responsibilities. According to the European Commission, harmonised strategies can lead to better risk management and incident response, reducing vulnerabilities across the Union's digital landscape [24]. Furthermore, shared policy frameworks enable faster information-sharing and joint operations, which are essential for responding to cross-border cyber incidents. A unified policy approach allows for more efficient resource allocation and streamlined communication channels, thereby enhancing collective security. Improved coordination among E.U. member states can significantly reduce response times during incidents, ensuring a quicker and more effective counter to cyberattacks. A fragmented policy landscape, however, can lead to disjointed efforts, ultimately weakening collective defence measures across the E.U. [35].

Resource allocation remains a critical challenge in bridging the gap between civilian and defence cybersecurity capabilities. Civilian agencies frequently struggle with budget constraints that limit their ability to invest in advanced cybersecurity technologies and maintain robust defences against sophisticated threats. Conversely, the defence sector, while generally well-resourced, may lack the agility and innovation-driven culture typical of the civilian tech industry. Strategic investment and funding mechanisms, such as the European Defence Fund and Horizon Europe, are crucial in addressing these disparities by supporting joint projects that leverage dual-use technologies applicable to both civilian and military contexts. Pooling resources and adopting shared funding initiatives can lead to more efficient use of technology and expertise, thereby enhancing the E.U.’s overall resilience against cyber threats. Furthermore, sustainable funding models are vital for the success of long-term cybersecurity projects; reliance on short-term funding can create vulnerabilities, leading to gaps in capability and preparedness that adversaries may exploit. Consistent and strategic financial backing is essential for developing enduring cybersecurity frameworks that can adapt to evolving threats.

Table 1. Detailed Key Challenges and Strategic Solutions for E.U. Civilian-Defence Cybersecurity Integration

Key Challenges	**Strategic Approach**	**Implementation Mechanism**	**Necessary Resources**
Fragmented civilian - defence policy frameworks	Develop cohesive E.U.-wide policy frameworks	Introduce civilian-defence synergistic policy initiatives under the E.U. Cybersecurity Strategy and Strategic Compass	Policy expertise, coordination across member states, funding for policy integration
Differences in operational cultures	Foster cross-sectoral collaboration through training and joint exercises	Create joint training programmes funded by Horizon Europe	Funding for joint exercises, trainers, facilities for simulation-based training
Resource allocation disparities	Implement strategic funding allocation for joint projects	Leverage European Defence Fund and Horizon Europe to support innovation	Financial backing from E.U. funds, investment in R&D, public-private partnerships
Regulatory inconsistencies	Harmonise regulations across civilian and defence sectors	Adopt E.U.-level directives and guidelines to standardise legal frameworks	Legal expertise, regulatory bodies, E.U. legislative support
Information-sharing barriers	Establish secure and standardised information-sharing protocols	Develop interoperable platforms and secure channels for data exchange	Secure communication technologies, cybersecurity standards, monitoring tools
Skills gap in cybersecurity workforce	Enhance education and training to build a versatile workforce	Collaborate with academic institutions for skill development programmes	Partnerships with universities, funding for scholarships and training, access to experts
Integration of emerging technologies	Promote ethical investment in dual-use technologies	Establish research partnerships to explore and deploy emerging tech solutions	Research grants, ethical guidelines, collaboration with tech firms and labs

To address these challenges (see the Table 1) member states should prioritise the establishment of unified command structures that bring together representatives from both civilian and defence sectors. Such entities could oversee the coordination of joint exercises, the sharing of intelligence, and the development of integrated response strategies to cyber incidents. This approach requires national and E.U.-level commitment to ensure consistency and avoid jurisdictional conflicts. Moreover, addressing the skills gap across the E.U. is imperative. Member states should implement cross-sectoral training programmes that include both civilian and military cybersecurity experts, building a workforce capable of handling complex cyber threats. Simulation-based exercises, for example, would prepare both sectors to manage hybrid threats, enhancing situational awareness and response capabilities.

A systematic approach to information-sharing must also be developed. Standardised protocols for sharing information between civilian and defence entities are essential to ensure a swift and coordinated response to cyber incidents. The NIS Directive has laid an important foundation in this regard, mandating cooperation among national cybersecurity agencies. However, further efforts are needed to streamline these protocols across sectors and member states, reducing response times and mitigating the impact of attacks.

Emerging technologies such as AI, machine learning, and quantum computing are reshaping the cybersecurity landscape, offering advanced tools for threat detection, prediction, and mitigation that can benefit both civilian and defence sectors. For example, AI-powered algorithms can process large datasets to identify patterns indicative of a cyber threat, enabling proactive measures before an attack is executed. Similarly, quantum cryptography promises unprecedented encryption capabilities, crucial for securing military and civilian communications. By investing in the development and

deployment of these technologies, member states can strengthen their cybersecurity capabilities across sectors. However, it is crucial that these investments are underpinned by policies that ensure the ethical use of emerging technologies and prevent their misuse for malicious purposes.

6. Conclusions

In the contemporary intricate security environment, the integration of civilian and defence sectors within the E.U.'s cybersecurity framework has emerged as a strategic imperative due to the increasingly complex and evolving nature of digital threats. This paper has argued that a systematic approach to strengthening civilian-defence cybersecurity synergy is crucial for effectively addressing both conventional and emerging threats, thereby ensuring the security and resilience of national and collective E.U. interests. The rationale for this integration is grounded in the interconnectedness of modern digital infrastructures, where disruptions can trigger cascading effects across multiple sectors, affecting both civilian and national security dimensions.

One of the primary findings of this research is the necessity for coordinated policy efforts across E.U. member states. Fragmented national policies and regulatory inconsistencies can lead to inefficiencies, creating exploitable gaps in defence measures. Harmonising policy frameworks, as exemplified by initiatives such as the E.U. Cybersecurity Strategy and the E.U. Strategic Compass, is critical to fostering cooperation between civilian and defence entities. Such coordinated efforts allow for more efficient resource allocation, streamlined communication, and improved incident response, thereby enhancing the overall security posture of the E.U.

This paper has also highlighted the significant challenges posed by differences in operational cultures between civilian and defence sectors. While the defence sector often operates under strict protocols of secrecy, the civilian sector prioritises transparency and open communication. Bridging this divide requires not only regulatory harmonisation but also the establishment of joint training programmes and unified command structures. These mechanisms can facilitate better cooperation, information-sharing, and the development of integrated response strategies that leverage the strengths of both sectors.

Resource allocation remains a critical challenge. Civilian agencies often face budget constraints that limit their ability to adopt cutting-edge technologies, while the defence sector, despite having more resources, may lack the innovation-driven approach typical of civilian tech industries. Strategic funding through mechanisms such as the European Defence Fund and Horizon Europe can address these disparities by supporting joint projects that utilise dual-use technologies. Effective investment strategies, coupled with sustainable funding models, are essential for building enduring cybersecurity frameworks capable of adapting to the dynamic threat landscape.

Additionally, the importance of addressing the skills gap within the E.U.'s cybersecurity workforce cannot be understated. The development of cross-sectoral training programmes, in collaboration with academic institutions, will help build a versatile workforce equipped to handle complex cyber threats. Moreover, the integration of emerging technologies, including AI, machine learning, and quantum computing, offers new opportunities for enhancing cybersecurity capabilities across both civilian and defence domains. However, ethical considerations must guide the investment and deployment of these technologies to prevent misuse.

Overall, this paper underscores that achieving a robust and integrated cybersecurity framework requires a holistic approach that considers policy, regulatory, financial, and technological dimensions. Member states must work collectively to address these challenges, drawing on both national and E.U.-level initiatives to create a cohesive and resilient cybersecurity ecosystem. Strengthening civilian-defence synergy will not only bolster the E.U.'s defensive capabilities but also reinforce its position as a global leader in cybersecurity innovation, safeguarding digital infrastructure, economic interests, and national security against a broad spectrum of cyber threats.

Future research could explore more in-depth case studies of successful civilian-defence integration within the E.U. and assess the long-term effectiveness of current policy frameworks. Such studies would contribute to understanding the practical implications of the strategic approaches discussed in this paper and provide further insights into optimising the E.U.'s cybersecurity resilience.

References

[1]. S. Walt, "The Origins of Alliances," Cornell University Press, 1987.
[2]. A. Wolfers, "National Security as an Ambiguous Symbol," Political Science Quarterly, vol. 67, no. 4, 1952, pp. 481-502
[3]. J. Mearsheimer, The Tragedy of Great Power Politics, New York: W.W. Norton, 2001.
[4]. B. Buzan, People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era, 2nd ed., Hertfordshire: Harvester Wheatsheaf, 1991.
[5]. L. Kello, The Virtual Weapon and International Order, New Haven: Yale University Press, 2017.
[6]. J. Nye, "Cyber Power," Harvard Kennedy School Belfer Center for Science and International Affairs, 2011.
[7]. Romania National Security Strategy, 2010.
[8]. Romania National Defence Strategy, 2020-2024.
[9]. NATO, "NATO Recognizes Cyberspace as a Domain of Operations," 2016.
[10]. DiCicco, Jonathan M., and Tudor A. Onea. "Great-Power Competition." *Oxford Research Encyclopedia of International Studies.* 31 Jan. 2023; Accessed 14 Oct. 2024.
[11]. P.W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford: Oxford University Press, 2014.
[12]. Thomas F. Lynch III, Introduction, In National Defense University, "Strategic Assessment 2020: Into a New Era of Great Power Competition," National Defense University Press, Washington, D.C., 2020. [Online]. Available: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2404286/1-introduction/. [Accessed: 13-Oct-2024].
[13]. F. G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars," Potomac Institute for Policy Studies, Arlington, VA, USA, 2007.
[14]. S. Reeves, "Hybrid Warfare: The Changing Character of Conflict and the Implications for International Humanitarian Law," *International Law Studies*, vol. 95, 2019, pp. 323-358.
[15]. R. Connolly, *Russia's Response to Sanctions: How Western Economic Sanctions Reshape Domestic Politics in Russia*, Cambridge: Cambridge University Press, 2018.
[16]. J.A. Lewis, "The Islamic State and Information Technology," in *Cybersecurity and Cyberwarfare: What Everyone Needs to Know*, 2020, pp. 141-155.
[17]. D. Wright, *Cybersecurity in the Internet of Things*, Cham: Springer International Publishing, 2019.
[18]. M. Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," 2018.
[19]. *Darktrace*, "Autonomous Response: AI Cyber Defense for Real-Time Threat Mitigation," Darktrace, 2023. [Online]. Available: https://www.darktrace.com. [Accessed: 14-Oct-2024].
[20]. *NATO CCDCOE*, "Locked Shields: NATO's Annual Cyber Defence Exercise," Cooperative Cyber Defence Centre of Excellence, 2023. [Online]. Available: https://ccdcoe.org. [Accessed: 14-Oct-2024].

[21]. *IBM*, “DeepLocker: How AI Can Power a Stealthy New Breed of Malware,” IBM Research Blog, Aug. 2018. [Online]. Available: https://www.ibm.com/blogs/research/2018/08/deeplocker/. [Accessed: 14-Oct-2024].
[22]. *National Institute of Standards and Technology*, “Post-Quantum Cryptography: NIST's Efforts to Secure the Future,” NIST, 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/post-quantum-cryptography. [Accessed: 14-Oct-2024].
[23]. *European Commission*, "The EU’s Cybersecurity Strategy for the Digital Decade," 2020.
[24]. *European Union Agency for Cybersecurity (ENISA)*, "ENISA Threat Landscape 2023," 2023.
[25]. *Eurostat*, "Cybersecurity and Trust in the Digital Economy," 2021.
[26]. A. Kaspersen, "Digital Sovereignty and Europe’s Role in Global Cybersecurity," *J. Eur. Cybersecurity Stud.*, vol. 5, no. 2, pp. 23-34, 2020.
[27]. *European Union Agency for Cybersecurity (ENISA)*, "The Cybersecurity Act", 2019.
[28]. *European Commission*, "Digital Europe Programme: A New Era of Cybersecurity", 2021.
[29]. *European Commission*, "A Strategic Compass for Security and Defence", 2022.
[30]. *Maritime Cybersecurity Centre of Excellence*, "ECYBRIDGE Project," [Online]. Available: https://ecybridge.eu/. [Accessed: 14-Oct-2024].
[31]. *European Commission,* "Permanent Structured Cooperation (PESCO)," [Online]. Available: https://www.pesco.europa.eu/. [Accessed: 20-Oct-2024].
[32]. *European Commission,* "European Defence Fund (EDF)," [Online]. Available: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en. [Accessed: 20-Oct-2024].
[33]. *European Research Executive Agency,* "Increased cybersecurity," [Online]. Available: https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/increased-cybersecurity_en. [Accessed: 20-Oct-2024].
[34]. R. Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies*, vol. 35, no. 1, pp. 5-32, 2012.
[35]. J. F. Dunn Cavelty and M. Wenger, "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics," *Contemporary Security Policy*, vol. 41, no. 1, pp. 5-32, 2020.
[36]. *European Parliament*, “Digital sovereignty for Europe,” 2020.