EU CyberNet

Navigating Complexity: Terminology, Taxonomy and Security in the Cyber-related Environment

- Dr. Damjan Štrucl

EU CyberNet Expert Series
No 2
2025

about

Damjan Štrucl

Dr. Štrucl is a researcher at the CCDCOE with over 25 years of expertise in information and cybersecurity. He has authored numerous articles, regularly serves as a panelist at international conferences and occasionally lectures at the Baltic Defence College. His work and research focus on cyber-related terminology, security taxonomy, hybrid warfare, information operations, critical infrastructure protection and the application of international law.

He has been part of the EU CyberNet Expert Pool since April 2021.

summary

Unified terminology plays a critical role in facilitating clear communication across scientific disciplines and bridging the gap between theory and practice. By offering a shared language that is widely understood, it eliminates confusion, enhances collaboration, ensures consistency and builds trust among experts and organisations. This becomes even more essential when addressing modern security threats linked to information and communication technology or modern technology, which we largely associate with cyberspace, space and electromagnetic spectrum. Effectively responding to such threats demands a holistic, interdisciplinary approach that integrates the technical aspects of modern technology into political, strategic and operational frameworks. Establishing a unified cyber-related terminology and security taxonomy helps to bridge the gaps between technical, operational and strategic levels, both nationally and internationally.

Introduction

The advancement of modern technologies and the emergence of new threats have fundamentally transformed the concept of security, extending beyond national borders and necessitating a unified global response. This evolving security landscape highlights the need for mutual understanding among stakeholders across political, strategic, operational and technical domains. However, a critical issue persists: the lack of clarity in cyber-related security taxonomy and terminological inconsistencies. Terms like 'cybersecurity' and 'information security' are often used interchangeably, reflecting the absence of a standardised taxonomy. Furthermore, while discussions on cyber resilience persist, the equally vital aspect of business continuity frequently goes unnoticed.

Emerging concepts – including the cyberspace-space nexus, the cyber electromagnetic environment and the information and communication technology (ICT) environment – further complicate this domain. These inconsistencies in terminology and understanding hinder the effectiveness of response strategies and undermine collective security efforts. An analysis of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) exercises and courses has shown that practitioners struggle to translate technical language into legal, strategic or operational terms, and vice versa. Another challenge is the unclear definition of roles and responsibilities in responding to severe cyber incidents, which becomes even more pronounced in international settings.

This raises a crucial question: does the current approach adequately address modern threats, and do we truly share a common understanding in national and international discussions despite using the same terminology? On the global stage, where cyber threats transcend national borders, achieving a unified and coordinated response is more critical than ever.

Futter and Štrucl highlight that the absence of universal definitions and concepts poses significant challenges to the application of international law and impedes cooperation among states.[1] Noor further notes that inconsistent terminology has complicated the operations and decision-making processes of the Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG), as evidenced in their reports.[2] Both groups prefer the term '(ICT) Environment' over 'cyberspace', which adds to terminological ambiguity in addressing cyber-related challenges. Importantly, we are not asserting that the term 'ICT Environment' is incorrect, but rather that its lack of clear definition allows for varied interpretations among general readers and experts from different disciplines. This issue is particularly pronounced on the international stage, where the term 'environment' in English may carry distinct meanings in various languages. Document A/76/136 of the UN General Assembly further underscores these differing understandings of the ICT environment and cyberspace.[3]

The challenges mentioned above highlight some of the difficulties decision-makers encounter in an evolving and dynamic security landscape. Simultaneously, new concepts such as the cyberspace-space nexus or cyber and electromagnetic space are emerging, shaped by the technical aspects of ICT. Due to these technical characteristics, addressing modern threats comprehensively is essential and this paper aims to provide such a holistic approach.

> *Inconsistent terminology affects national cybersecurity strategies and hinder cohesive global approaches to cybersecurity and defence.*

An overview of cyber-related security taxonomy and terminology

A uniform and widely understood cyber-related terminology and set of concepts are crucial for advancing global efforts in cybersecurity, cyber defence and resilience, as well as for the development of international law. Experts, including those from the European Union Agency for Cybersecurity (ENISA), Noor and Klimburg, have emphasised the challenges posed by inconsistent terminology, which affect national cybersecurity strategies and hinder cohesive global approaches to cybersecurity and defence. However, a shared vocabulary does not automatically ensure mutual understanding, as cultural, historical and linguistic differences – particularly in translations – can distort meaning and impede effective communication.[4] Additionally, the varied interpretations of terminology lead to inconsistencies that create challenges at both international and national levels, affecting all operational tiers – from political-strategic to technical-tactical – and disrupting collaboration between public and private sectors as well as between security and defence entities.

> *Information security is data-centric and encompasses the protection of information across digital, electronic and physical domains, while cybersecurity is system-centric and focuses specifically on safeguarding digital systems, networks and data from cyberattacks.*

Although previous analyses, dating back to 2012 and 2020, highlight ongoing challenges, the situation remains unchanged, as evidenced by the CCDCOE study involving five international organisations and 12 member states.[5] The study revealed that while international organisations and most countries incorporate broader security concepts, such as Information Assurance and Information Security, they fail to integrate the existing cyber-related security taxonomy within their organisational frameworks. (Figure 1).

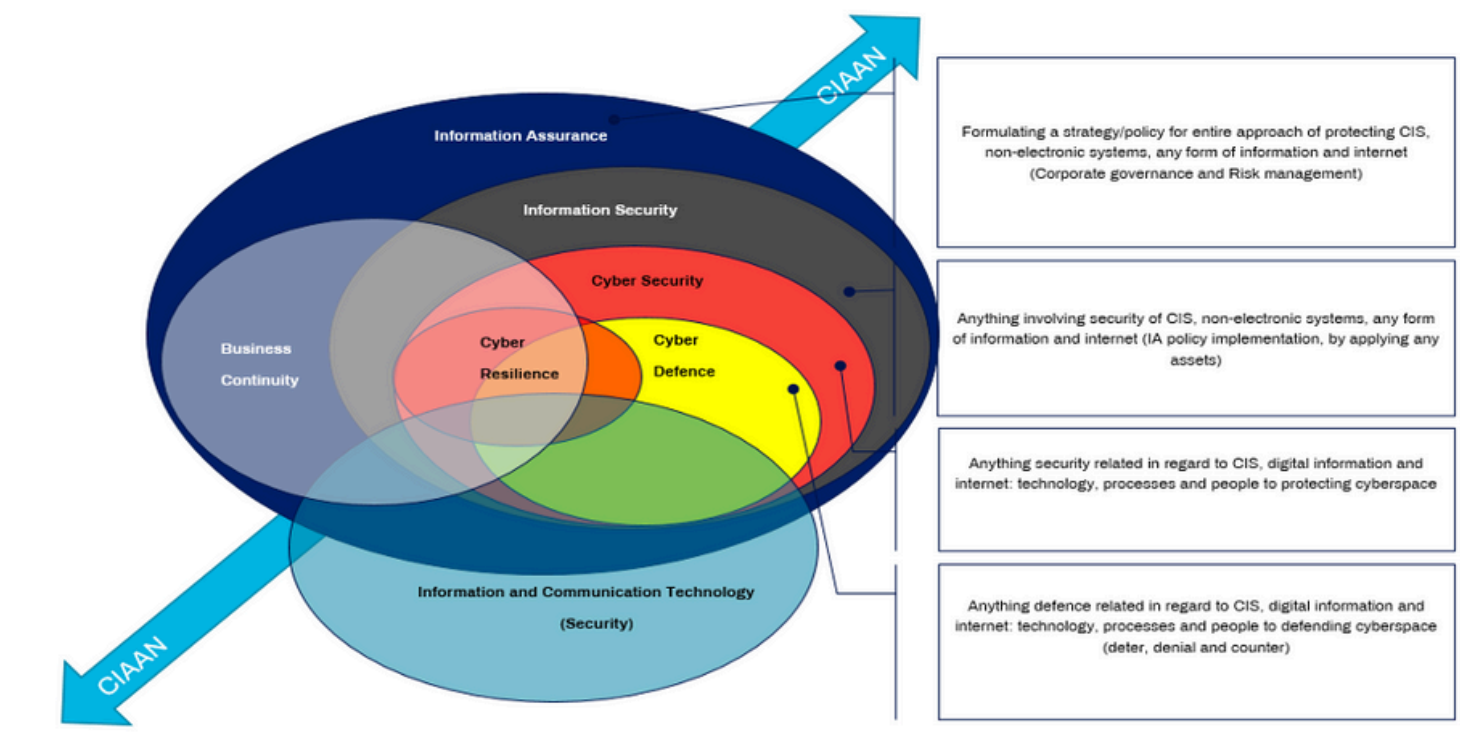

Figure 1: Generic enterprise security architecture of the security of communication and information systems[6]

Additionally, experts have observed that information security and cybersecurity are often used interchangeably, with some countries and organisations mistakenly equating the two – a fundamentally flawed approach. Information security, unlike cybersecurity, is data-centric and encompasses the protection of information across digital, electronic and physical domains. It includes measures such as physical, technical and environmental safeguards, access control and cybersecurity, all aimed at securing sensitive data and organisational systems from misuse, unauthorized access, disruption or destruction.[7] In contrast, cybersecurity is system-centric and focuses specifically on safeguarding digital systems, networks and data from cyberattacks.[8]

The CCDCOE study revealed that nearly half of the countries surveyed employ their own definitions, even though these nations are both EU and NATO members. A minority of countries adopt definitions based on ISO or NIST standards. (Chart 1) This diversity in definitions does not imply inadequacy but reflects varying perspectives, which contribute to inconsistent approaches to global cybersecurity. Furthermore, it is important to note that terms like 'protection', 'security' or 'defence' may be interpreted differently depending on an individual's profession (e.g. soldiers, police officers) or field of expertise (e.g. technical or social sciences).

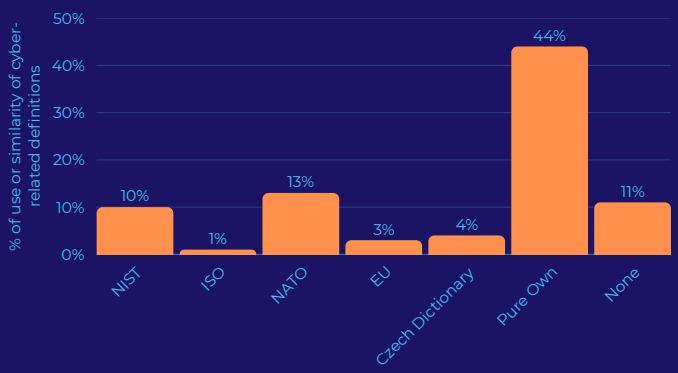

Chart 1: Use or similarity of states' definitions with organisations' definitions[9]

> *Countries continue to independently develop military cyber capabilities in alignment with NATO while simultaneously building civilian capabilities to protect critical infrastructure in accordance with EU standards, often overlooking the cyber-related security taxonomy or hybrid threat environment.*

Different approaches of NATO and EU member states

In 2016, NATO's Cyber Defence Commitment marked a pivotal step in international efforts to address cyber challenges, setting the stage for subsequent NATO-EU joint declarations and annexes.[10] These agreements emphasised the need for building mutual trust between NATO and EU member states through information sharing and collaborative initiatives to strengthen cybersecurity, resilience and defence. However, there is disagreement among individual countries and NATO regarding the EU's classification of information security as a subset of cybersecurity. Additionally, the EU's approach diverges from ISO standards, while NATO aligns with NIST standards. These differing perspectives and definitions are reflected in the diverse cybersecurity and defence strategies adopted by various countries.

Most nations are also developing military cyber capabilities, which tend to have no utility during in peacetime. This division into strictly civilian or military approaches reduces the effectiveness of national systems for responding to cyber and hybrid threats, despite the interconnected nature of the information environment and cyberspace. Additionally, many countries heavily invest in military cyber capabilities that, according to their policies, remain largely unused during

peacetime due to the role of armed forces in such periods. Differences in understanding national cybersecurity concepts further complicate efforts to achieve a unified global approach.

Although building trust and fostering a shared understanding of cyber-related concepts – such as information assurance and information security – seems straightforward, [11] implementation is challenging due to the intricate nature of the information environment and cyberspace. National security strategies and international perspectives highlight the borderless nature of cyberspace and the transnational scope of threats. Strong military cyber capabilities are being developed but often remain unused during peacetime, even though strategic strength lies in promoting connectivity rather than separation. While it is true that the role of the armed forces in peacetime is limited, it is also crucial to acknowledge that the information environment and cyberspace are not entirely divisible into military and civilian parts. Nevertheless, countries continue to independently develop military cyber capabilities in alignment with NATO while simultaneously building civilian capabilities to protect critical infrastructure in accordance with EU standards, often overlooking the cyber-related security taxonomy or hybrid threat environment. This is especially important from the perspective of Russia, which does not officially define cyberspace, but instead uses the term 'information sphere'.[12] This parallel development results in duplication of staff and resources, as well as two different perspectives on ensuring security or confronting hybrid threats.

> *Two critical factors must be addressed: the shared information and communication architecture connecting these domains – enabled by ICT through EMS and the Internet – and the predominant ownership by the civilian sector*

Different perspectives on cyber-related environment

Instead of concluding, it is more effective to chart a clear path forward for resolving the terminological dilemma. The foundation for addressing security threats in the information environment, cyberspace and the electromagnetic spectrum (EMS) lies in ICT. In practice, it is crucial to consider the dual-use nature (military and civilian) of the information environment and cyberspace, where various state and non-state actors operate. Porche outlines the information environment as comprising three interconnected dimensions – Information, cognitive and physical – linked through ICT. This environment is shaped by the relationship between space and cyberspace, which facilitates interactions among communication and information systems (CIS), data, individuals and organisations. (Figure 2) [13]. Moreover, the dependence of cyberspace on EMS is fundamental. Creedon underscores the significance of the connection between space and cyberspace, emphasising their reliance on shared technical capabilities and the mutual threats enabled by ICT and EMS.[14] Consequently, Haig and others advocate replacing the term 'cyberspace' with 'cyber electromagnetic domain' to better reflect this integration,[15] a change adopted by Switzerland.[16]

The information environment serves as the primary domain for hybrid operations or 'grey zone' activities that remain below the threshold of armed conflict or aggression, highlighting the necessity of defining the role of armed forces even during peacetime. Moreover, the dual-use nature of the information environment, cyberspace, space, ICT, EMS and the Internet calls for a nuanced approach to their governance and security. Two critical factors must be addressed: the shared information and communication architecture connecting these domains – enabled by ICT through EMS and the Internet – and the predominant ownership by the civilian sector.[17] These concepts cannot be

adequately defined without considering their technical characteristics, nor can military cyber operations be effectively executed without civilian sector support. The defence sector heavily relies on the connectivity provided by Internet service providers, which restricts the cyberspace available to defence forces.

> *Not every ICT-related incident qualifies as a cyber-incident; however, all ICT-related incidents are, by definition, information security incidents.*

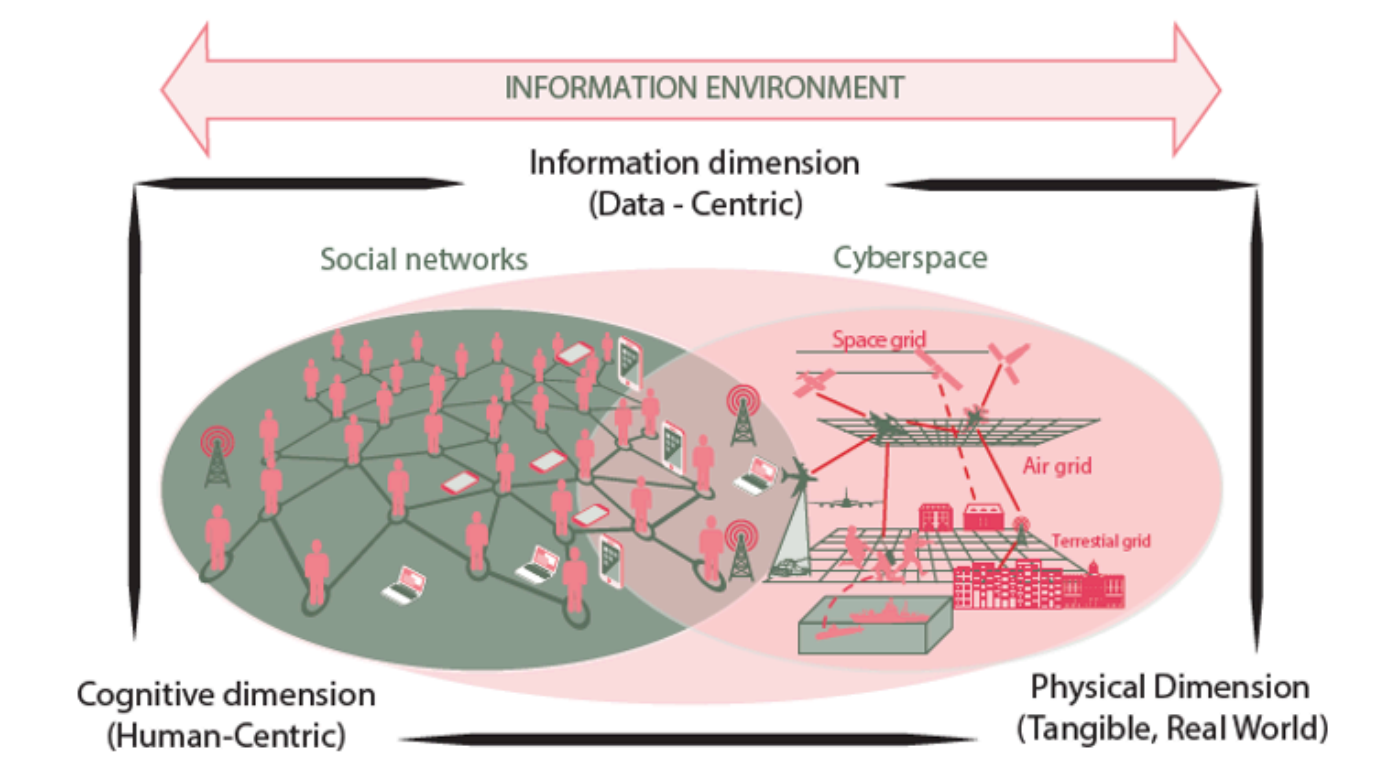

Figure 2: Information Environment[18]

From theory to practice: the way forward

Both in theory and practice, a fundamental challenge persists at all levels – the ability to comprehend the modern security environment, in which ICT and EMS play a central role. Unfortunately, most academics, politicians and decision-makers primarily associate this environment with hybrid and cyber threats while overlooking the technical characteristics of ICT. Not every ICT-related incident qualifies as a cyber-incident; however, all ICT-related incidents are, by definition, information security incidents – a distinction that is frequently ignored.

From a technical perspective, this differentiation may not pose a major issue, as ICT experts prefer focus on safeguarding Critical Information Systems (CIS) and protecting digital and electronic data rather than debating terminology. However, at political, strategic and operational levels – where key decisions on national and international security policies are made – clearly defining cyber-related security and standardising terminology is crucial. To create a cohesive framework for cyber or ICT-related security taxonomy and terminology, several key points must be considered:

1. Technical Perspective: The Information Environment, Cyberspace and Space are inherently interconnected through a shared EMS and ICT infrastructure. Additionally, the Information Environment and Cyberspace

rely on Internet Service Providers (ISPs), which, from a national standpoint, serve as gateways to the global digital and electronic ecosystem. In this context, the International Telecommunication Union (ITU) and international standardisation bodies play a vital role in translating technical language into strategic and operational terms – and vice versa.

2. Strategic Perspective: Armed forces cannot conduct cyber operations independently without ISPs, making them reliant on civilian infrastructure. Similarly, civilian entities alone cannot effectively counter hybrid threats, necessitating a closer alignment between military and civilian security strategies. Despite significant resource allocations for military cyber capabilities, many nations lack clearly defined roles for their armed forces in this domain. In addition, decision-makers need to take into account the growing role of international ICT-related companies, whose products impact national and global security. Therefore, the EU and NATO should take the lead in proposing an integrated civil-military and public-private approach to address modern threats effectively.

3. Policy Integration Perspective: Given the technical nature of ICT and EMS, it is essential to establish a hierarchy of strategies rather than focusing solely on cybersecurity and defence strategies. A truly comprehensive approach should encompass the technical, strategic, legal, social, economic and defence dimensions of the information environment, cyberspace, space and EMS. It is therefore an interdisciplinary approach involving a range of experts who are directly and indirectly involved in the implications of modern threats with/through the use of ICT. In addition, policies need to be set to regulate cooperation (even beyond economic benefits) with national and transnational ICT-related companies and to establish minimum ICT security standards. The EU serves as an example of good practice in this regard, as it has already introduced partial regulations prescribing minimum ICT security standards.

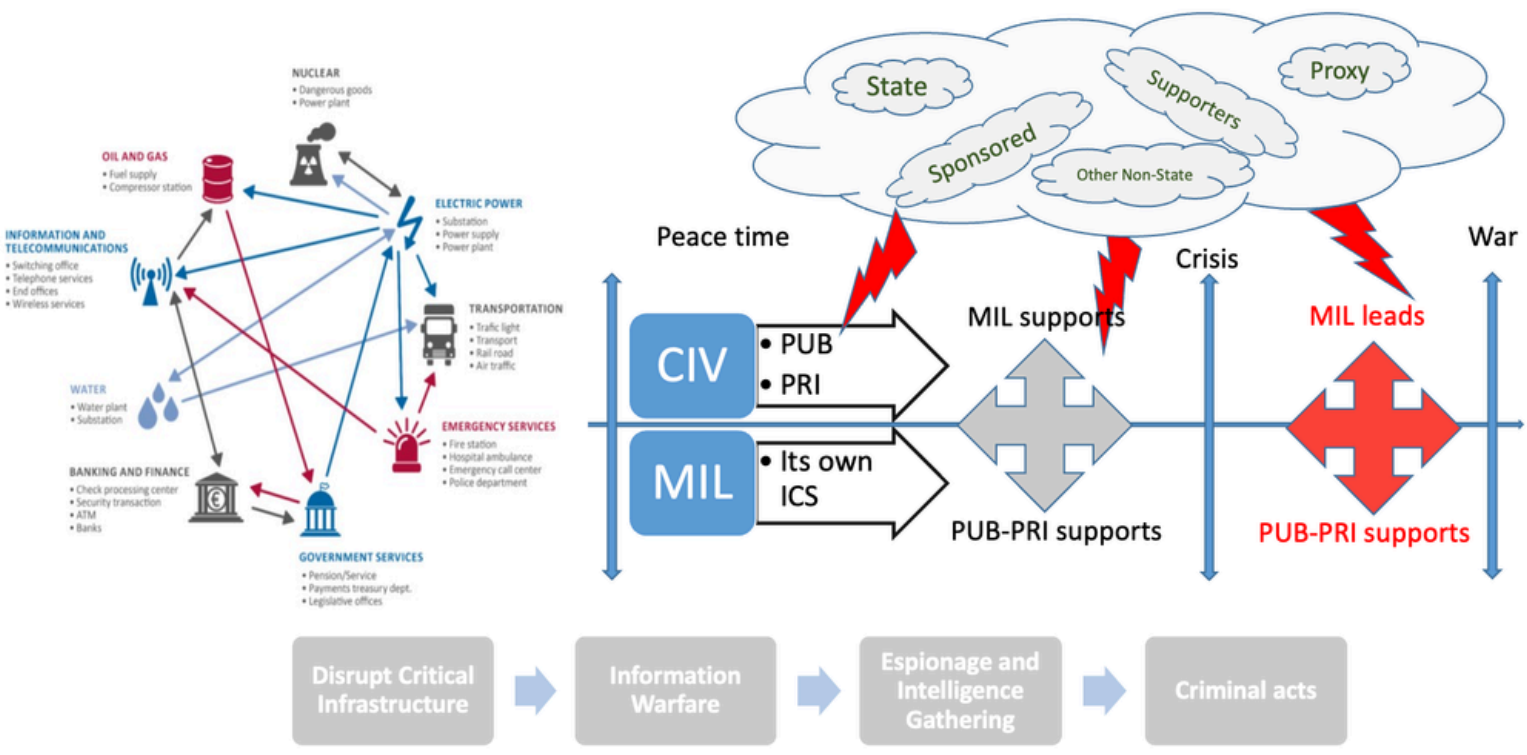

Figure 3: Integrated Approach – from peace to war [19]

This debate inevitably raises important questions about the roles and responsibilities in addressing contemporary ICT challenges. Solutions may vary in scope, from national to international levels and in complexity. Regardless of the approach, subject-matter experts must play a crucial role in guiding national and international decision-makers, helping them navigate the complexities of the issue while bridging academic knowledge with practical experience.

This highlights the need to transition from a multidisciplinary approach to an interdisciplinary one, both nationally and internationally. The EU and NATO are well-positioned to lead this effort, as CCDCOE's experience indicates that Asian and South American countries most frequently seek the sharing of best practices and methodologies from these two entities.

References

[1] Futter, A., 2018. Journal of Cyber Policy: 'Cyber' semantics: why we should retire the latest buzzword in security studies, Vol. 3, No.2. Taylor & Francis Group
Štrucl D., 2020. Contemporary Military Challenges: Terminology confusion in ensuring cyberspace security, Vol.22, No. 4, October 2020

[2] Noor, E. 2021. Tallinn Winter School of Cyber Diplomacy, 2021. Ministry of Foreign Affairs of Estonia. Retrieved 22. 11. 2024, from https://www.youtube.com/watch?v=bxWGc4Db7Z4

[3] UN General Assembly, A/76/136, 2021. Refer to examples illustrating diverse interpretations of the term 'ICT Environment' in the Official Compendium of Voluntary National Contributions. This document addresses how international law applies to the use of ICT by States, as submitted by governmental experts participating in the GGE on Advancing Responsible State Behaviour in Cyberspace (73/266). Document A/76/136, retrieved 12. 05. 2024, from https://documents.un.org/doc/undoc/gen/n21/189/48/pdf/n2118948.pdf

[4] Štrucl, D., 2022. Comparative study on the cyber defence of NATO Member States, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

[5] Štrucl, D., 2022. Comparative study on the cyber defence of NATO Member States, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

[6] Štrucl, D., 2022. Comparative study on the cyber defence of NATO Member States, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

[7] Microsoft. (2024). What is information security (InfoSec)? Retrieved 11 29, 2024, from https://www.microsoft.com/en-us/security/business/security-101/what-is-information-security-infosec

Štrucl, D., 2022. Comparative study on the cyber defence of NATO Member States, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

[8] Microsoft. (2024A). An overview of cybersecurity. Retrieved 11 29, 2024, from https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity

[9] Štrucl, D., 2022. Comparative study on the cyber defence of NATO Member States, p.60, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

[10] Le Gleut, R, Conway-Mouret, H, 2019. Information report No. 626. France: Working Group on European Defence, p. 19-20

[11] Klimburg, A., 2012. National Cyber Security Framework Manual. Tallinn: NATO CCDCOE Publication, p. 9
Falessi, N., Gavrila, R., Klejnstrup, M. R., & Moulinos, K., 2012. National Cyber Security Strategies. Practical Guide on Development and Execution. Heraklion: ENISA, p. 1

[12] Временной комиссии по развитию информационного общества Совета Федерации Федерального Собрания Российской Федерации, 2014. In 2014, the Temporary Commission on the Development of the Information Society of the Federation Council of the Federal Assembly of the Russian Federation drafted the Concept of the Cybersecurity Strategy of the Russian Federation. Retrieved 30. 11. 2024, from http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

[13] Porche III, R. I., 2016. Emerging Cyber Threats and Implications. Santa Monica: RAND. Additionally, information environment is a strategic battleground for state and non-state actors, spanning political, economic and military conflicts – from grey-zone tactics to full-scale war – where cyber operations and electronic warfare (EW) mutually enhance each other (Porche III, R. I. et al., 2013)

[14] Creedon, M. R., 2012. Space and Cyber: Shared Challenges, Shared Opportunities. Strategic Studies Quarterly. Vol. 6, No. 1, 3-9

[15] Haig, Z. (2015). Electronic Warfare In Cyberspace. Security and Defence Quarterly Vol. 2, Issue 7, DOI: 10.5604/23008741.1189275, pp. 22-35

[16] Schweizerische Eidgenossenschaft, 2022. Gesamtkonzeption Cyber: Konzeption der Weiterentwicklung der Fähigkeiten der Schweizer Armee im Cyber- und elektromagnetischen Raum bis Mitte der 2030er-Jahre. Retrieved 12 12, 2024, from https://www.newsd.admin.ch/newsd/message/attachments/78655.pdf

[17] Some major countries have their own navigation and communications satellites, so they can carry out cyber activities independently

[18] Porche III, R. I., 2016. Emerging Cyber Threats and Implications. Santa Monica: RAND

[19] Štrucl, D., 2024. Cyberspace as a Domain of Operations, ILOCOC course, CCDCOE

Navigating Complexity: Terminology, Taxonomy and Security in the Cyber-related Environment
Dr. Damjan Štrucl

EU CybetNet Expert Series, No 2, 2025

EU CyberNet

Funded by the European Union