CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Comparative study on the cyber defence of NATO Member States

Damjan Štrucl

NATO CCDCOE Strategy Researcher

Tallinn 2021

About the author

Lieutenant Colonel Dr Damjan Štrucl is an officer in the Slovenian Armed Forces and is currently a researcher in the Strategy Branch at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). He has been working in the field of communications and information systems since 2004. During his career, he was the Commander of the signal unit and an INFOSEC officer in several units of the Slovenian Army. From 2015 to 2020 he served as a senior officer of cyber defence and as the head of the Cyber Defence Department of the General Staff of the Slovenian Army. His research focuses on the comparative analysis of the legal and institutional regulations of cyber security (CS) and defence between countries and between NATO and the EU. He has completed several educational programmes and training courses on information and CS at home and abroad, holds a Master's degree in Governmental and European studies and a Doctorate in law from the New University, Slovenia.

Acknowledgements

The author would like to thank Dr Claire Kwan, Commander Jacob Galbreath and Commandant Rónán Micheal O’Flaherty for their thorough reviews and engagement with the topic.

CCDCOE

The NATO CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world’s largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring the Centre hosts the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. Since January 2018, CCDCOE has been responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by the following NATO nations and partners of the Alliance: Austria, Belgium, Bulgaria, Canada, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, the UK and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the NATO CCDCOE (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of the information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Table of Contents

1. Abstract

The information environment and cyberspace have created a completely different security environment than the one we are used to. With the help of communication and information systems, the world has become interconnected in real-time and threats are no longer limited to physical borders. New pitfalls have emerged which are reflected in different understandings of the contemporary security environment. Everything that happens in cyberspace is transferred to the physical environment, but it is never possible to know or predict exactly when this will happen. There is a different understanding of the modern security environment and this can cause the common approach and response by states to fail.

Cyber defence and cyber resilience are important parts of the measures taken by states and international organisations to ensure an adequate level of CS in national security systems. This paper reports the findings from a survey made with the CCDCOE Member Nations, NATO and EU organisations to better understand the approaches and capabilities of other like-minded states.

The study first analyses the terminology used and the strategic, legal and operational arrangements of the states, which will provide information on their approaches to CS and cyber defence. As a part of this analysis, it was found that states understand cyber-related terminology very differently and some states neglect the importance of information assurance or even understand it as information security. It is similar in the understanding of information security concerning CS, which can cause issues in the effective common response to contemporary security threats.

Secondly, the study focuses on the legal and institutional framework, organisational structure and capabilities of CS and cyber defence. It was found that states have a very different organisational infrastructure concerning CS or cyber defence, although most surveyed states are NATO and EU members. Because of that membership, no major deviations were expected, at least not in the legal framework as states should follow NATO's commitments and the EU's legal framework. However, it turned out differently as states do not follow uniform standards of NATO or EU.

Our scope is thus the assessment of a complete structure of cyber defence and interplay with national CS structures. This includes an organisational overview of responsibilities for cyber defence in which government entities are responsible for cyber critical aspects of critical infrastructure protection if there is a dedicated, centralised or coordinating government body or Ministry responsible for CS and cyber defence. Additionally, the analysis in capabilities, cooperation, collaboration and information sharing was conducted to get insight into over whole structure of CS and the cyber defence of states.

2. Introduction

The cyber domain has a great influence on the transformation of security concepts and the contemporary security environment has become more complex than ever as threats and challenges are no longer limited to national borders. Effective CS, cyber resilience and cyber defence require a common and comprehensive approach, for which the individual state is primarily responsible. International cooperation is required to contribute to national security and thus to global and regional security and cyber defence is no exception. Therefore, NATO emphasises the need to follow the 360-degree approach to the implementation of NATO Strategic Concept tasks which will address the entire operational space of all combat domains, including cyber effects.

In 2016, the NATO Commitment on Cyber Defence was signed, followed by two joint NATO-EU statements and two annexes.[1] NATO and EU States committed themselves to building mutual trust by sharing information and participating in various projects, while implementing national projects or initiatives to develop CS, cyber resilience and cyber defence. However, if states have different approaches and understandings for these important cyber-related concepts the question becomes, "how does the international community arrive at a common approach to address cyber-related challenges, risks, threats and insecurities?" The answer is in a way quite simple and concurrently difficult to implement. The first step towards the common approach should be the de facto implementation of trust between respective entities and the second step a common and uniform understanding of cyber-related concepts,[2] including information assurance and information security.[3]

The terminology confusion or different perceptions of concepts are reflected both in national security strategies[4] and in the international community. States and the international community should be aware that cyberspace is global; it knows no borders or physical spatial domains and the threats and risks have a transnational dimension. Today we face a complex threat environment in which threats and attacks are becoming more interconnected, sophisticated and damaging. Things that happen in cyberspace do not remain in cyberspace, but are transferred to other dimensions of space. Strategic power or advantage no longer lies in the state's military power or its geographical location, but rather in the information communication technology (ICT), knowledge and information. Since states do and never will have the same ICT, we can conclude that knowledge and information are power in the information and cyber environment. By sharing information, we share knowledge and thus common cyber-related concepts at both national and international levels can be adopted, which are the cornerstones of a common approach to ensure an appropriate level of CS, cyber resilience and cyber defence.

The CCDCOE Member States are mostly Member States of NATO, the EU or both. Therefore, the initial hypothesis is that states use are more or less uniform cyber-related concepts and develop cyber capabilities in the line with NATO-EU joint statements. Those concepts are precisely defined by NATO and the EU and the cyber-related concepts of both organisations are aligned and in the line with the concepts of international standardisation organisations.

The goal of this paper is the analysis and synthesis of information based on a review of professional and scientific articles, the definitions of international organisations and the responses received from CCDCOE Member States. It seeks to understand the differences in approaches to CS, resilience and defence and allows harmonising and improving current national and global CS, resilience and defence.

[1] Le Gleut and Conway-Mouret, 2019, p. 19.

[2] Klimburg, 2012, p. 9; Falessi et al, 2019, p. 1.

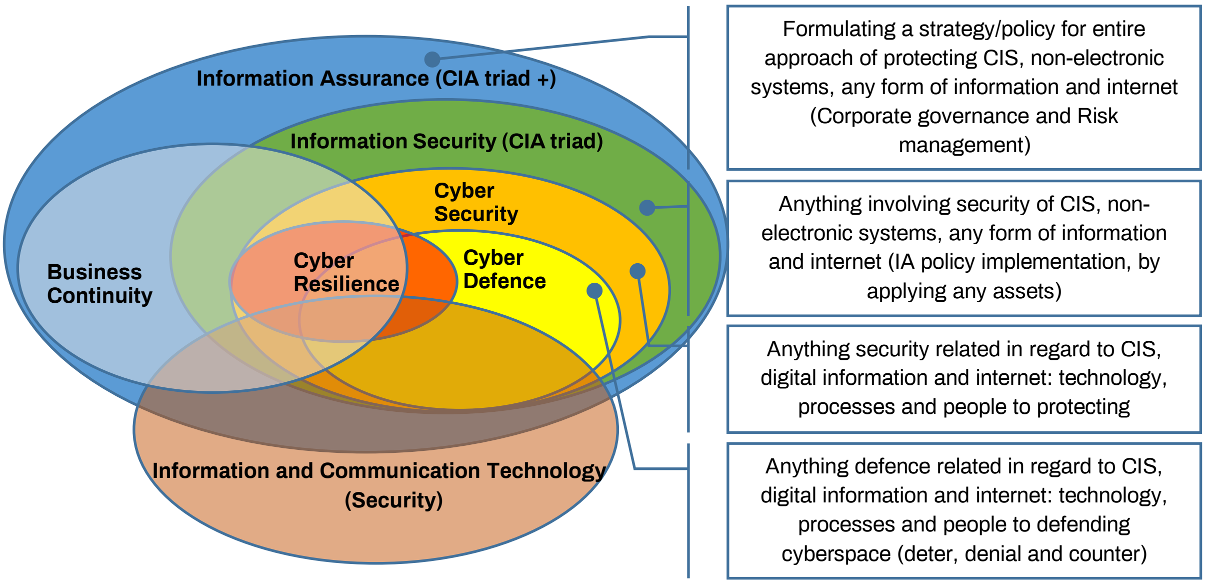
[3] Kosseff, 2018, p. 1001-1003.

[4] Klimburg, 2012, p. 8-30.

2.1 Research approach

At the request of Luxembourg, the CCDCOE was invited to obtain information on the organisation of CS and the defence of CCDCOE Member States. The original aim was to conduct a comparative study of various concepts, cyber defence maturity and capabilities to better understand the current national organisational cyber defence and CS structures and processes. The CCDCOE invited its Member States and partners to participate in the study. Sixteen out of the 34 States responded to the study, with four refraining from providing answers due to other commitments. Due to the lack of data, the original purpose of the study was changed into a comparative study focusing on high-level capabilities and the scene-setting of how respondents define various cyber-related concepts. Some states did not give their consent to the disclosure of their name and are therefore marked with 'State' and the corresponding number.

Recognising that public discussions are mostly about CS, cyber defence and cyber resilience, we opted for a comprehensive and holistic research approach to the security architecture of information and systems security. For effective CS and defence, the entire security architecture must be considered as security levels are inextricably linked. With a comprehensive approach, we have gained states' views on the understanding of the terminology related to the security of information and communication information systems. The definitions of the Institute of Electrical and Electronics Engineers (IEEE), the International Organisation for Standardisation (the ISO), the National Institute of Standards and Technology (NIST) and various academic and professional articles were used as references.


Information Assurance (CIA triad +)
Information Security (CIA triad)
Cyber Security
Business Continuity
Cyber Resilience
Cyber Defence
Information and Communication Technology (Security)

Formulating a strategy/policy for entire approach of protecting CIS, non-electronic systems, any form of information and internet (Corporate governance and Risk management)

Anything involving security of CIS, non-electronic systems, any form of information and internet (IA policy implementation, by applying any assets)

Anything security related in regard to CIS, digital information and internet: technology, processes and people to protecting

Anything defence related in regard to CIS, digital information and internet: technology, processes and people to defending cyberspace (deter, denial and counter)

Figure 1: Generic enterprise security architecture of an information and systems security[5]

The study also focused on basic ICT definitions as it is essential to know the difference between terms such as data, ICT and communication and information systems (CIS). The study thus contains two Appendixes: Appendix 1 is a collection of rudimentary definitions of cyber-related issues and Appendix 2 is a collection of the definitions of responders.

The second part of the study is aimed at the analysis of the security architecture and cyber capabilities of states regarding the information environment, focusing on the legal and institutional framework, including cyber capabilities and human resources. The analysis is based on the responses received from the states surveyed, where open answers regarding the security architecture are broken down into sub-elements of each answer and binary evaluated to reduce bias and gain consistency.

[5] Adapted from the ISO 27XXX; the ISO 22301; Appendix 1; Appendix 2.

2.2 Methodology

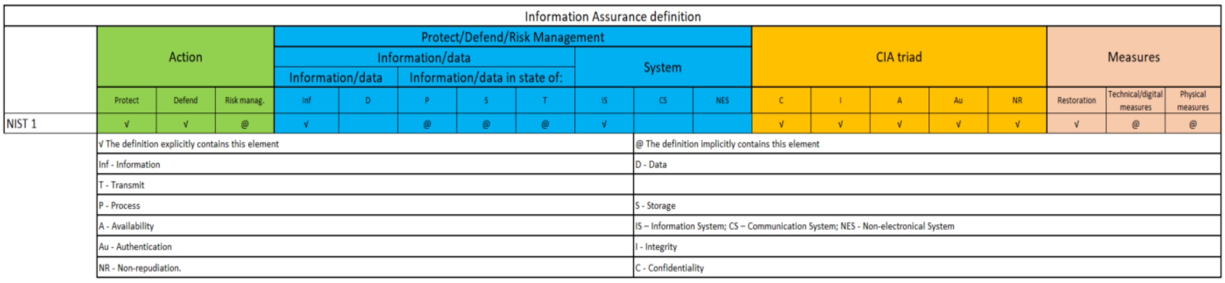
The concept of this study was based on the assumption that states' cyber-related concepts are in the line with the concepts of NATO and EU. However, their organisational architecture differs due to the various levels of CS development and national legislation. Therefore, the CCDCOE prepared two questionnaires[6] consisting of 86 binary, pre-coded and open-ended questions addressing terminology, legal (including the application of standards) and organisational frameworks, cooperation and information sharing, capabilities and human resources. To extract and analyse a set of data from the questionnaire, a comparative analysis was used. The analysis was based on a variable-oriented and case-oriented comparative strategy to describe and explain the similarities and differences of responders' cyber-related concepts and approaches to CS.

Comparative research design	Many-Entities comparison	Single Entity study
Comparative Strategy	Variable-oriented	Case-oriented
General Methodology	Quantitative	Qualitative

Figure 2: Comparative methodological choices

A case-oriented comparative strategy was used to obtain qualitative results regarding the cyber-related concepts of the respondents and their security architecture. Definitions of recognised standardisation organisations such as the UN, NATO and the EU were used as a basis for concept analysis. The definition was broken down into sub-elements and the elements evaluated as to whether an individual element was implicitly (marked with @) or explicitly (marked as √) used in the definition, allowing us to evaluate the definition qualitatively and quantitatively (Figure 3). A military and academic approach to understanding the content of the concepts was used. However, the reader may feel that some sub-elements have not been properly evaluated with 'explicit' and 'implicit' as it depends on whether the reader is military or civilian or a native speaker or foreigner.

The variable-oriented comparative strategy was used to obtain the quantitative results regarding the uniformity of cyber-related concepts and their security architecture. To reduce bias and to ascertain congruity and coherence among states' and organisations' definitions, we looked for differences between selected words in the composition of definitions and whether the definition was used verbatim by the state or not. The Merriam-Webster Dictionary was used to achieve consistency in the understanding of selected words and ideas.



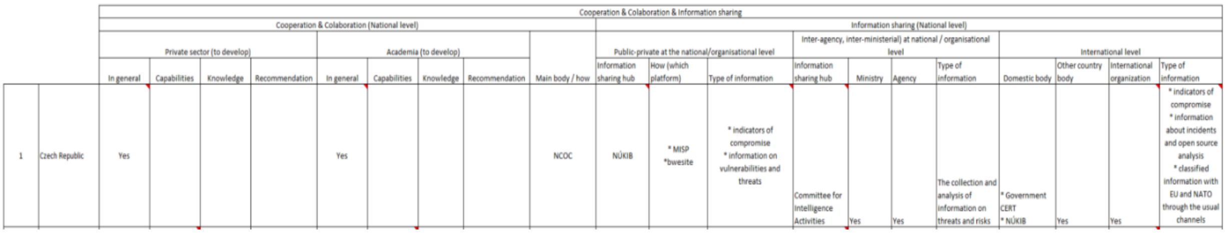
Information Assurance definition																			
	Action			Protect/Defend/Risk Management								CIA triad					Measures		
				Information/data					System										
				Information/data		Information/data in state of:													
	Protect	Defend	Risk manag.	Inf	D	P	S	T	IS	CS	NES	C	I	A	Au	NR	Restoration	Technical/digital measures	Physical measures
NIST 1	√	√	@	√		@	@	@	√			√	√	√	√	√	√	@	@

√ The definition explicitly contains this element	@ The definition implicitly contains this element
Inf - Information	D - Data
T - Transmit	
P - Process	S - Storage
A - Availability	IS – Information System; CS – Communication System; NES - Non-electronical System
Au - Authentication	I - Integrity
NR - Non-repudiation.	C - Confidentiality

Figure 3: An example of a definition broken down into sub-elements

[6] The questions in part A were designed to collect data on cyber-related concepts and to gain general insights to organisational and/or institutional framework. The part B of the questionnaire was designed to collect more sensitive data, such as cyber offensive capabilities, future cyber capabilities, human resources, etc.

Open answers were evaluated according to the identification of the required elements in the imposed question. The comparisons were to determine whether differences in CS approaches exist between states while evaluating as many of the sub-elements of the legal and standards framework, organisational framework, cooperation and information sharing framework, capabilities and human resources as possible (Figure 4). The aim was to harmonise states' approaches to CS as the focus was on commonalities and a common core of CS and defence approaches. The study provides a comprehensive overview of the security maturity and cyber defence capabilities and which cyber-related concepts and standards the states follows (ISO, NIST, others).



		Cooperation & Colaboration & Information sharing																			
		Cooperation & Colaboration (National level)									Information sharing (National level)										
		Private sector (to develop)				Academia (to develop)					Public-private at the national/organisational level			Inter-agency, inter-ministerial) at national / organisational level				International level			
		In general	Capabilities	Knowledge	Recommendation	In general	Capabilities	Knowledge	Recommendation	Main body / how	Information sharing hub	How (which platform)	Type of information	Information sharing hub	Ministry	Agency	Type of information	Domestic body	Other country body	International organization	Type of information
1	Czech Republic	Yes				Yes				NCOC	NÚKIB	* MISP *bwesite	* indicators of compromise * information on vulnerabilities and threats	Committee for Intelligence Activities	Yes	Yes	The collection and analysis of information on threats and risks	* Government CERT * NÚKIB	Yes	Yes	* indicators of compromise * information about incidents and open source analysis * classified information with EU and NATO through the usual channels

Figure 4: An example of broken down open question

3. Findings

A systematic approach to the analysis showed that the states did not answer the questions in full, so we performed a comparative analysis of only those sub-elements to which the states most fulsomely responded. By doing so, we have assured a greater level of objectivity.

The report shows the disparity in the common understanding of some definitions, but this does not mean that these definitions are less good. The blue colour in the charts shows the number of states or sum of implicitly evaluated sub-elements, and orange is the corresponding percentage or sum of explicitly included sub-elements. Some states refrained from answering certain questions, which will be mentioned in the subchapters where this occurred.

3.1 Cyber-related concepts – Terminology

Uniform and professional terminology or its common understanding is crucial for global progress in ensuring effective CS, cyber defence and cyber resilience, and for the development of international law. The problem of a lack of common understanding was pointed out by European Union Agency for Cyber Security (ENISA), Klimburg and other experts and is reflected in national CS strategies and the global approach to CS and defence.[7]

However, the problem of non-uniform terminology can also be non-uniform understanding as it does not follow that if we all speak the same language, we also understand it equally. This is especially reflected in translations where understanding can lose its meaning, especially due to cultural and historical differences.

For an objective assessment of the definitions of states, we used the Merriam-Webster Dictionary and Appendix 1, based on which we marked the sub-elements with implicitly (marked as √) included or explicitly (marked as @) stated. This differentiation shows the extent to which the understanding of the content of the definition is left to the reader.

This chapter will summarise the findings regarding 11 cyber-related concepts (Appendix 2) drawn from the responses to Part A of the questionnaire. Chart 1 shows the number of accepted or understood definitions by states and organisations. However, some definitions were not analysed (Cyber Offensive and Defensive Operations, Critical Infrastructure - CRI, Communication and Information System Critical Infrastructure – CIS CRI, Hybrid Operations - HO, Information Operations - IO) and some do not apply to the UN (Information Assurance, Information Security, Cyber Security) and the ISO.[8] (Cyber Operation). In addition, the Czech Republic refrained from providing definitions related to cyber operations.

[7] ENISA, 2012, p. 9; Klimburg, 2012, p. 9; Schatz, D et al., 2017, pp 53-54; Futter et al., 2018, p. 201; Falessi et al., 2019, p. 1; Štrucl, 2020, pp. 32-33.

[8] Information Assurance, Information Security, CS, Cyber Operation.

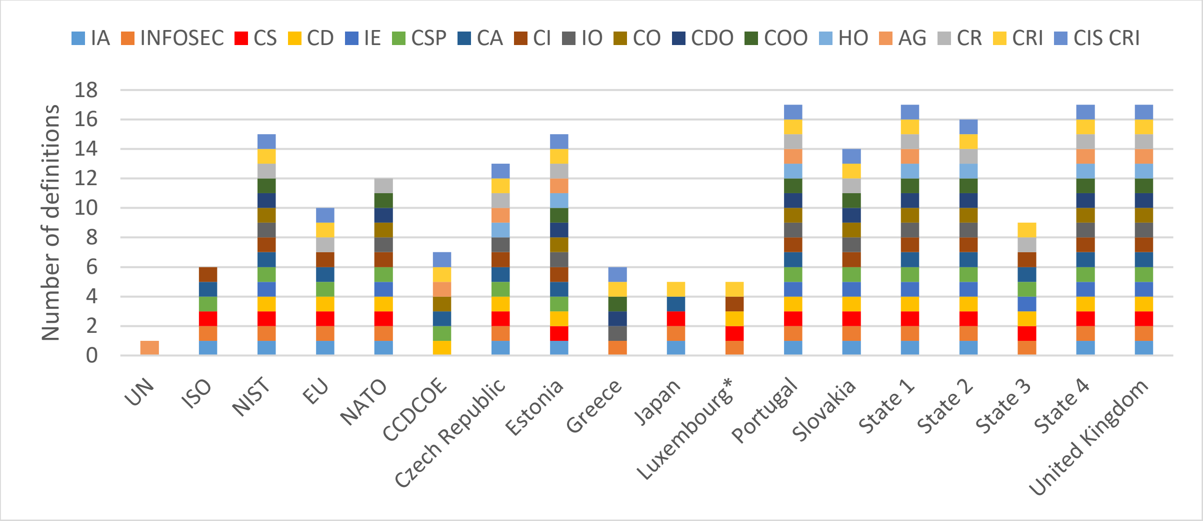


Chart 1: Summary of States' and Organisations' definitions

3.1.1 Information assurance

Information Assurance[9] (IA) is often understood as a concept that is not security related to CIS.[10] This is certainly not the case as from a holistic point of view IA is the basis for the protection of all types of information and systems.[11] In general, IA means the measures and activities of an organisation, ensuring that their critical information and systems are secure and protected and that the legitimate users get the right information at the right time.[12] Therefore, IA is a strategically-oriented function focusing on the strategic (business) security design (management, protection and defence) of all critical systems and information by ensuring their availability, integrity, authentication, confidentiality and nonrepudiation.

According to Joint Force Command (JFC), the IA is the blueprint for information superiority and, together with Cyber Operations (CO), supports Information Operations (IO).[13] JFC is aware that missing or inadequate IA policy can jeopardise any critical information and systems, and so the ability to provide reliable and secure information in support of any mission should be established.[14] This is especially important nowadays with global connectivity and automated processes where the imperative is to understand and mitigate strategic risks and to exchange information instantaneously among states and partners. Therefore, an IA policy (security design) should be in place covering governance, security planning, strategic risk management, auditing of assets, certification and accreditation of electronic systems.

To be able to evaluate the IA concept, we divided it into sub-elements: the actions within the IA concept, its measures and the elements that need to be protected. Table 1 shows the understanding of IA among respondents and an overview of the differences in IA concepts between them. Research and analysis have shown that the ISO deals only with strategic risk management, four entities do not have any definitions, while NATO has two definitions. The most commonly explicit covered sub-elements are 'protect', 'information', 'Information System' and 'CIA triad +' (Confidentiality, Integrity, Accessibility, Authentication and Nonrepudiation), which is consistent with the general understanding of IA. However,

[9] NCI Agency is NATO body providing Information Assurance expertise to NATO partners and allies. (NCIA, 2021, e-source)

[10] Knapp, 2009, p. 295. CIS includes Communication and information technology, people, processes, information/data, hardware and software (Appendix 1; Tuovinen & Frilander, 2019, p. 36).

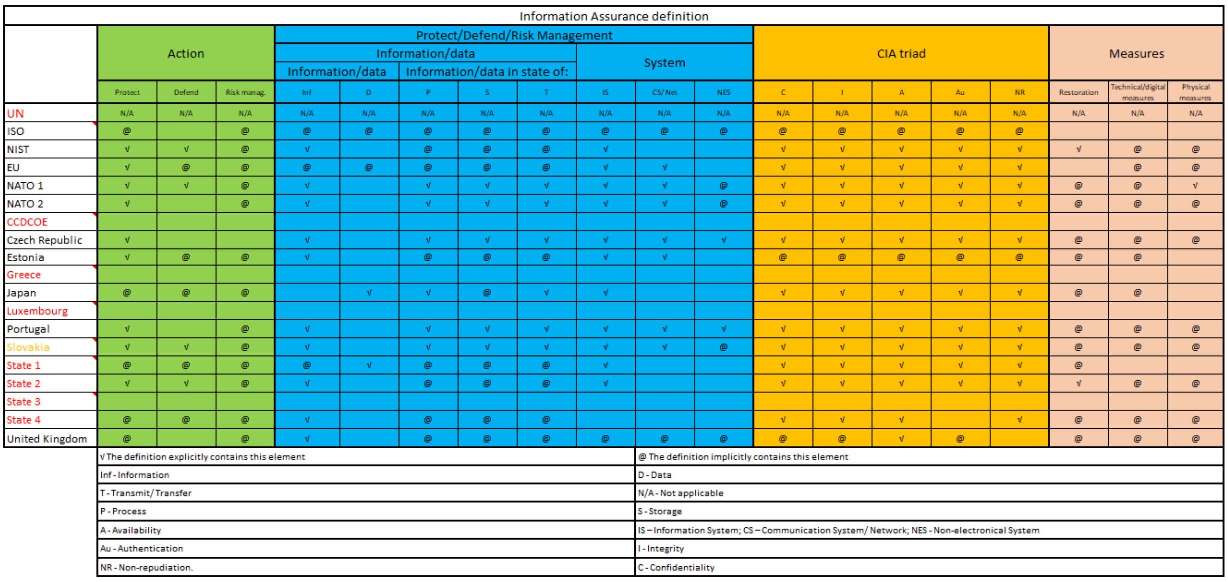
[11] Schou & Hernandez, 2015, pp. 14-16.

[12] Knapp, 2009, p. 284; Klump, 2018, e-source; MacLeod, 2015, p. 52.

[13] Joint Publication 3-13, 2014, pp. I-8; Joint Publication 6, 2019, pp. I-6.

[14] MacLeod, 2015, p. 52.

the omission of communication systems and networks and non-electronic systems from the definitions are inconsistent with the general understanding of IA. In addition, instead of protecting information, some entities have defined data[15] in a general sense, although the underlying IA function is to determine what data is information and what value that information has. The protection of all data is very wasteful in terms of resource consumption, so only the value of the data needs to be protected.



Information Assurance definition																			
	Action			Protect/Defend/Risk Management								CIA triad					Measures		
				Information/data					System										
				Information/data		Information/data in state of:													
	Protect	Defend	Risk manag.	Inf	D	P	S	T	IS	CS/ Net	NES	C	I	A	Au	NR	Restoration	Technical/digital measures	Physical measures
UN	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
ISO	@		@	@	@	@	@	@	@	@	@	@	@	@	@	@			
NIST	√	√	@	√		@	@	@	√			√	√	√	√	√	√	@	@
EU	√	@	@	@	@	@	@	@	√	√		√	√	√	√	√		@	@
NATO 1	√	√	@	√		√	√	√	√	√	@	√	√	√	√	√	@	@	√
NATO 2	√		@	√		√	√	√	√	√	@	√	√	√	√	√	@	@	@
CCDCOE																			
Czech Republic	√			√		√	√	√	√	√	√	√	√	√	√	√	@	@	@
Estonia	√	@	@	√		@	@	@	√	√		@	@	@	@	@	@	@	
Greece																			
Japan	@	@	@		√	√	@	√	√			√	√	√	√	√	@	@	
Luxembourg																			
Portugal	√		@	√		√	√	√	√	√	√	√	√	√	√	√	@	@	@
Slovakia	√	√	@	√		√	√	√	√	√	@	√	√	√	√	√	@	@	@
State 1	@	@	@	@	√	@	@	@	√			√	√	√	√	√	@		
State 2	√	√	@	√		@	@	@	√			√	√	√	√	√	√	@	@
State 3																			
State 4	@	@	@	√		@	@	@				√	√	√		√	@	@	@
United Kingdom	@		@	√		@	@	@	@	@	@	@	@	√	@		@	@	@

√ The definition explicitly contains this element	@ The definition implicitly contains this element
Inf - Information	D - Data
T - Transmit/ Transfer	N/A - Not applicable
P - Process	S - Storage
A - Availability	IS – Information System; CS – Communication System/ Network; NES - Non-electronical System
Au - Authentication	I - Integrity
NR - Non-repudiation.	C - Confidentiality

Table 1: Comparative analysis definition of the information assurance

Table 1 shows that the NATO 1 and NIST definitions are similar as the same actions (protection and defence) on the same elements (information systems, information) are included. However, the included elements are no longer the same as NATO also includes elements of physical security. So, the IA concept or idea of both organisations is the same, but the elements of measures to implement it are different.

There are also differences between the explicit and implicit content of sub-elements as shown in Table 1 and Chart 2. The sum of implicitly and explicitly included elements shows us the total value of an individual entity concept. Several entities explicitly include 'defence' as a necessary action and some as an implicit one, while risk management is included only implicitly, although it should be the underlying element of the IA concept. In addition, some entities have an agnostic approach or such a general definition that everyone can understand in their own way. Thus in most entities' definitions, it is left to the reader to evaluate each concept, how he understands the definition, how he evaluates each concept and what actions or security measures need to be designed under IA. This is reflected in the replies of the Czech Republic, which replied that it did not see a difference between IA and information security (INFOSEC)[16] or Japan and State 1, which replied that the definition was not defined at the national level; they did define an understanding of the IA concept. However, the reader's understanding of a given definition may not be the same as the entity whose definition it is.

[15] Data is raw material of facts and figures, while information is interpreted data with the meaning. (Appendix 1)

[16] NATO uses the abbreviation INFOSEC, referring only to the information security of CIS. (Appendix 2)

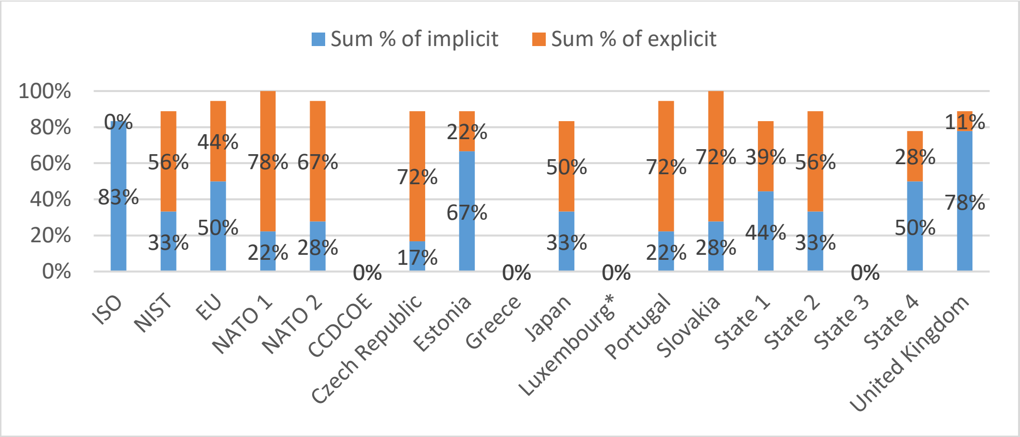
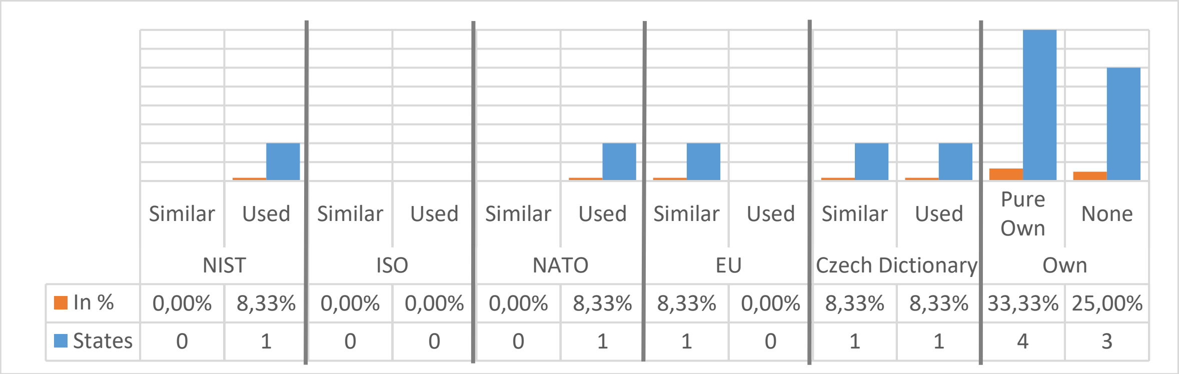


Chart 2: Explicit/ implicit included elements in the definition of information assurance

A comparison of the coherence of the definitions between the surveyed states and organisations is shown in Chart 3. This assessment is based on an analysis of concepts where NATO's goal is to protect and defend information, ICS and the non-electronic system by ensuring the CIA+ triad, while the EU's goal is to have confidence that this system will protect information. Some states only include maintaining or ensuring the CIA+ triad. Chart 3 shows that only two states use NATO (Slovakia) and NIST (State 2) definitions verbatim, two have similar definitions to the EU (Estonia) and Czech dictionaries (Portugal), the Czech Republic uses its own dictionary, four have their own understanding of the IA concept and three do not have an IA concept at all. Thus there is no coherence between the definitions of states and organisations and their understanding of the IA concept may differ.



	NIST		ISO		NATO		EU		Czech Dictionary		Own	
	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Pure Own	None
■ In %	0,00%	8,33%	0,00%	0,00%	0,00%	8,33%	8,33%	0,00%	8,33%	8,33%	33,33%	25,00%
■ States	0	1	0	0	0	1	1	0	1	1	4	3

Chart 3: Similarity of 'IA' definitions according to organisations' dictionaries

3.1.2 Information security

While IA refers to a comprehensive strategy and practice related to information assurance and risk management to protect the integrity of information, INFOSEC is a set of policies, tools and practices for protecting and defending all information and the system from illicit access (Figure 5). INFOSEC, as a subset of IA, focuses on the implementation of IA policy to ensure business continuity and minimise business damage by the development and implementation of security measures (physical, technical, organisational and personal, etc.), tools and techniques to keep information safe and secure.[17] Thus, in the general sense, IA is the collection and evaluation of information to mitigate overall risks and INFOSEC is how to keep that information secure by ensuring the integrity, confidentiality and availability (CIA triad – security requirements) of the CIS from all kinds of threats. In general, authentication and nonrepudiation

[17] Solms & Van Niekerk, 2013, p. 98.

are not indirectly implied in INFOSEC as those two attributes have been already covered by IA (a legitimate user gets the right information).[18]

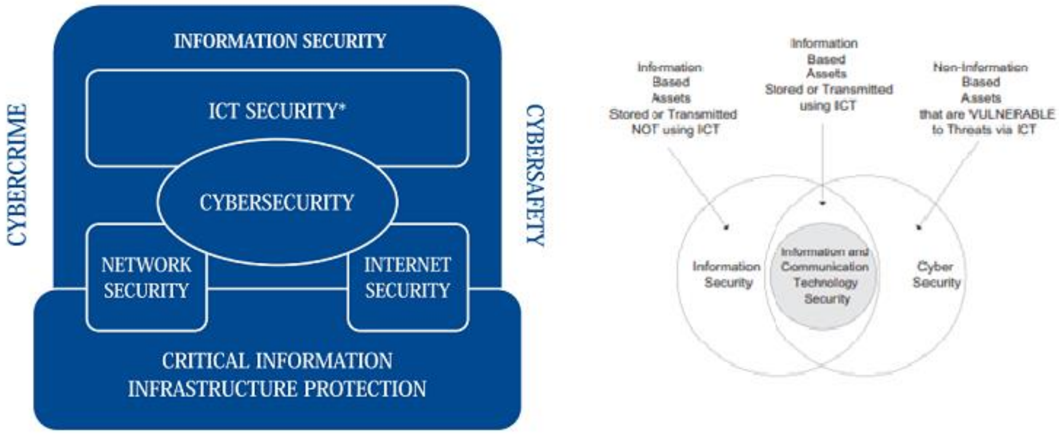

INFORMATION SECURITY
ICT SECURITY*
CYBERSECURITY
NETWORK SECURITY
INTERNET SECURITY
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION
CYBERCRIME
CYBERSAFETY
Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are 'VULNERABLE to Threats via ICT
Information Security
Information and Communication Technology Security
Cyber Security

Figure 5: The relationship between information and communication security, information security and CS[19]

In the CIA triad context, INFOSEC is responsible for all forms and types of information and systems of the organisation against unauthorised disclosure, access, processing, use, storage, transfer, alteration or destruction.[20] Both concepts deal with the protection and defence of all information and systems, but IA covers policy on strategic risk management and identifies the valuable assets which need to be protected, while INFOSEC focuses on implementing IA policy and business continuity by use of processes, tools, technologies and techniques designed and deployed to achieve IA goals and to mitigate threats and vulnerabilities against assets.[21]

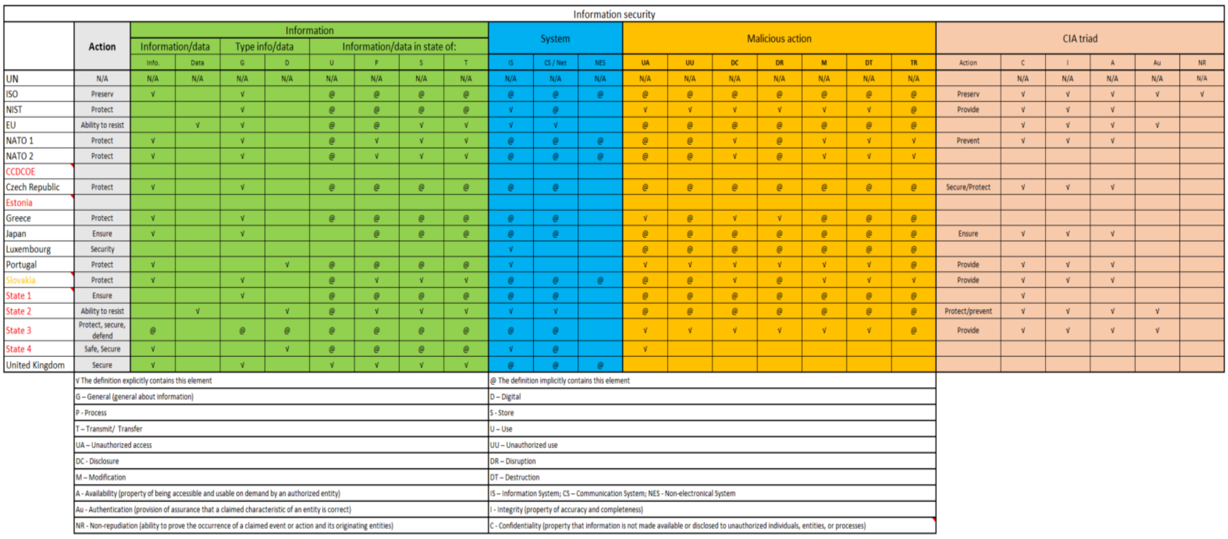
The analysis of the concepts of INFOSEC is shown in Table 2. To evaluate the INFOSEC concept, we have divided it into sub-elements following the traditional approach to providing INFOSEC: actions within the INFOSEC concept, malicious actions and elements that need to be protected. Two of the 18 entities do not have any definition, while NATO has two. Most entities consider the sub-element 'information' in a general sense, which is in line with the general understanding of the INFOSEC concept. However, they omit non-electronic systems. The most common actions related to 'information and system' are 'protect' and 'secure', while most common actions related to the CIA triad are 'provide' or 'prevent' and 'protect'. Such a diversity of words used can be understood very differently, especially in the relationship of the military to civilian conception. In addition, some entities defined data protection in the general sense instead of information protection, although the basic function of INFOSEC is the implementation of the IA concept; that is, safeguarding of information or value of data.

[18] Schou & Hernandez, 2015, pp. 15-16; Sosin, 2018, pp. 47-49.

[19] Solms & Van Niekerk, 2013, p. 101, Klimburg, 2012, p. 10.

[20] Schou & Hernandez, 2015, p. 16; NIST, Glossary, 2021, e-source; SANS, 2021, e-source.

[21] INFOSEC includes: Information Security Management System (ISMS), Security Information and Event Management (SIEM) (Tuovinen & Frilander, 2019, pp. 43 – 45), networks, servers and software configuration, custom security appliance and off-the shelf operation systems configuration, custom intrusion detection, and digital forensics (Klump, 2018).



Information security																									
	Action	Information								System			Malicious action							CIA triad					
		Information/data		Type info/data		Information/data in state of:																			
		Info.	Data	G	D	U	P	S	T	IS	CS / Net	NES	UA	UU	DC	DR	M	DT	TR	Action	C	I	A	Au	NR
UN	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A		N/A	N/A	N/A	N/A	N/A
ISO	Preserv	√		√		@	@	@	@	@	@	@	@	@	@	@	@	@	@	Preserv	√	√	√	√	√
NIST	Protect			√		@	@	@	@	√	@		√	√	√	√	√	√	@	Provide	√	√	√		
EU	Ability to resist		√	√		@	@	√	√	√	√		@	@	@	@	@	@	@		√	√	√	√	
NATO 1	Protect	√		√		@	√	√	√	@	@	@	@	@	√	@	√	√	√	Prevent	√	√	√		
NATO 2	Protect	√		√		@	√	√	√	@	@	@	@	@	√	@	√	√	√						
CCDCOE																									
Czech Republic	Protect	√		√		@	@	@	@	@	@		@	@	@	@	@	@	@	Secure/Protect	√	√	√		
Estonia																									
Greece	Protect	√		√		@	@	@	@	@	@		√	@	√	√	@	@	@						
Japan	Ensure	√		√			@	@	@	@	@		@	@	@	@	@	@	@	Ensure	√	√	√		
Luxembourg	Security									√			@	@	@	@	@	@	@						
Portugal	Protect	√			√	@	@	@	@	√			√	√	√	√	√	√	@	Provide	√	√	√		
Slovakia	Protect	√		√		@	√	√	√	@	@	@	@	@	√	@	√	√	√	Provide	√	√	√		
State 1	Ensure			√		@	@	@	@	@	@		@	@	@	@	@	@	@		√				
State 2	Ability to resist		√		√	@	√	√	√	√	√		@	@	@	@	@	@	@	Protect/prevent	√	√	√	√	
State 3	Protect, secure, defend	@		@	@	@	@	@	@	@	@		√	√	√	√	√	√	@	Provide	√	√	√	√	
State 4	Safe, Secure	√			√	@	@	@	@	√	@		√												
United Kingdom	Secure	√		√		√	√	√	√	@	@	@													

√ The definition explicitly contains this element	@ The definition implicitly contains this element
G – General (general about information)	D – Digital
P - Process	S - Store
T – Transmit/ Transfer	U – Use
UA – Unauthorized access	UU – Unauthorized use
DC - Disclosure	DR – Disruption
M – Modification	DT – Destruction
A - Availability (property of being accessible and usable on demand by an authorized entity)	IS – Information System; CS – Communication System; NES - Non-electronical System
Au - Authentication (provision of assurance that a claimed characteristic of an entity is correct)	I - Integrity (property of accuracy and completeness)
NR - Non-repudiation (ability to prove the occurrence of a claimed event or action and its originating entities)	C - Confidentiality (property that information is not made available or disclosed to unauthorized individuals, entities, or processes)

Table 2: Comparative analysis definition of the information security

Table 2 shows that the definitions of entities differ according to the actions that the entities implement in their INFOSEC concept. More detailed findings are presented in Chart 5, which shows the differences between the explicit and implicit content of sub-elements. The sum of the implicitly and explicitly included elements shows the total value of each entity concept. However, the total value does not necessarily coincide with the entity's evaluation. Only seven of the 18 entities explicitly include the 'Information System' as an element to be protected and only two explicitly include the 'network'. There are also different approaches to protecting against malicious acts; only four explicitly include them, although this should be included by default as a basic element of the INFOSEC concept. Thus in most definitions, it is left to the reader how they understand the definition or which elements need to be protected, which measures need to be taken and against which malicious acts. This is shown by the replies of Estonia which stated that it would prefer to use the term CS instead of INFOSEC. In addition, several states have accepted a general definition of the term INFOSEC which can be understood in its own way, while State 1 has not defined INFOSEC at the national level but does have an understanding of the concept.

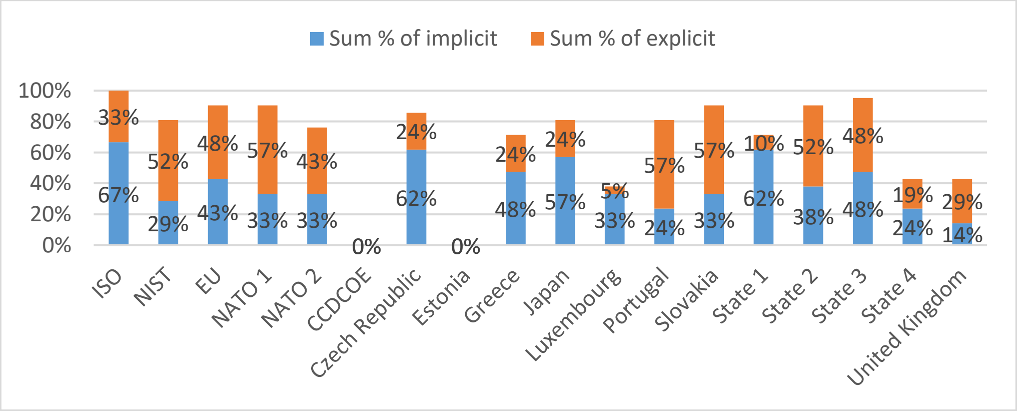


Chart 4: Explicit/ implicit included elements in the definition of information security

The different understandings of the INFOSEC concept are reflected in the coherence of the definitions between the surveyed states and organisations as shown in Chart 5. NATO's goal is to protect information, ICS and the non-electronic system against unauthorised disclosure, transfer, modification or destruction, while the EU's goal is the ability of a network or an Information System (IS) to resist. Unlike these organisations, some states' goals are to protect the CIA triad or information from unauthorised access and disclosure or the disruption of authorised access or the safe and secure use of the information. Only one state uses the NATO definition in verbatim (Slovakia), two (Portugal and State 3) have a similar definition to NIST, two have a similar definition to the ISO (Japan) or EU (State 2), and the Czech Republic uses its own national dictionary terminology.[22] Five states have their own understanding of the IA concept and one does not have an INFOSEC concept at all. Additionally, the EU advocates the INFOSEC concept as a subset of CS, which is contrary to the general understanding of the INFOSEC concept. There is thus no coherence between the definitions of states and organisations and their understanding of the IA concept may differ respectively.

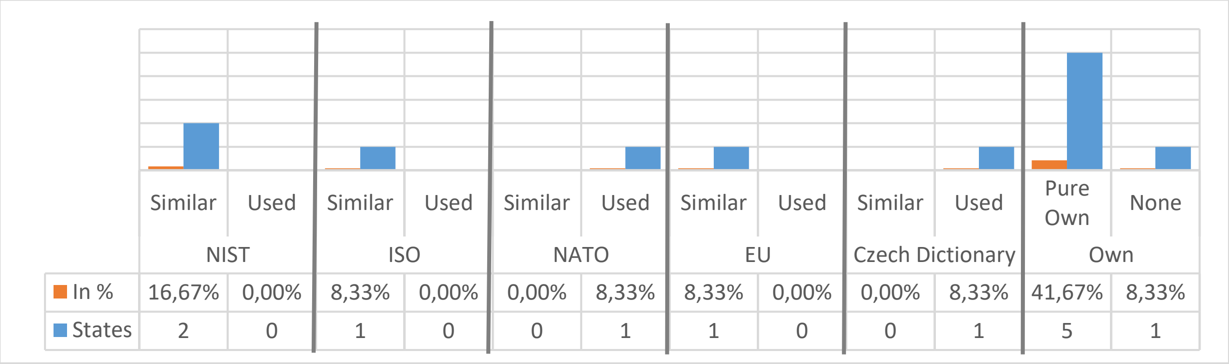


Chart 5: Similarity of 'INFOSEC' definitions according to organisations' dictionaries

3.1.3 Cyber security

CS is now one of the most commonly used terms in ensuring global security. The difference between cyber and information security is anything but clear, especially since the terms are often used interchangeably.[23] There are almost no academic or professional articles on this issue and many blogs cover either IS or CS that are similar in content. Despite the lack of literature and different ways to understanding concepts, two approaches have developed:

- Information security is obsolete as the landscape of threats has changed due to the emergence of new ICT and the internet and the shift to electronic business processes, therefore a conceptual shift is needed.
- Traditional approach to security by the holistic approach through the linear contribution of each definition. [24]

In general, most of the research results have the same outcome regarding INFOSEC vs. CS and that is:

- They are not interchangeable;
- Each includes strategies, policies, practices, concepts, techniques and tools to protect valued data and systems against threats and vulnerabilities;
- INFOSEC is the safeguard any type of information and assets regardless of realm, while CS is the protection of cyberspace; and
- The three pillars of INFOSEC are the CIA triad, but ensuring the triad is also the function of CS.
- INFOSEC protects any type of information or asset against unauthorised access, disclosure, modification, disruption or similar threats, while CS is the protection of cyberspace against cybercrime, cyber terrorism, cyber espionage and cyber attacks.[25]

[22] CS Glossary by National CS Centre of the Czech Republic, National Security Authority of the Czech Republic.

[23] Solms & Van Niekerk, 2013, p. 97; Schou & Hernandez, 2015, p. XXVIII; Althonayan & Andronache, 2018, p. 68.

[24] Althonayan & Andronache, 2018, pp. 68-69; Klump, 2018, e-source.

[25] Solms & Van Niekerk, 2013, pp. 98-101; Reid & Van Niekerk, 2014, p. 2; Schou & Hernandez, 2015, p. 16; Althonayan & Andronache, 2018, pp. 69-72.

Since the research failed to obtain a clear delineation between INFOSEC and CS, we made our own analysis to find differences between the two terms based on the discussed cyber-related concepts (Appendix 2) and web blogs. The main findings are as follows:[26]

INFOSEC	CS
The synergy of CS and information security.	
INFOSEC is a necessary measure of IA.	CS is a necessary measure of INFOSEC.
INFOSEC design processes that protect critical information and assets in any form.[27]	CS prevent INFOSEC processes to be compromised.
Primarily Off-the-shelf systems, access, compliance, procedurals and technical controls.	Off-the-shelf systems, emerging ICT, APTs.
Protect any type of critical information and assets from unauthorised user, access, disclosure, modification or similar threats to ensure CIA triad of any information.	To protect and keep digital data that underpins critical information and ICT secure against threats and vulnerabilities emanating from cyberspace to ensure the CIA triad of digital information.
Protect and defend any type of information and assets against unauthorised access, disclosure, modification or similar threats.	Protect and defend cyberspace against cyber threats (cybercrime, cyber terrorism and cyber attacks).
Protect any type of information and assets from any threat and vulnerabilities.	Protect and keep secure digital data and ICT from cyber threats and vulnerabilities.
Protect and preserve digital information that can be found on removable disks, laptops, personal devices and many other ICT.	Protect and secure digital data that can be accessed via vulnerabilities in its networks and systems and the internet.
Focusing on the future risk, threats and vulnerabilities.	Focusing on immediate risk and the ability to stop attacks that are happening now and seeking vulnerabilities to prevent future risks.

Table 3: Information security vs. CS

Many researchers and professionals use a sliding scale to delineate phases of the CS concept. As is shown in Figure 6, the CS concept encompasses five phases: architecture, passive defence, active defence, intelligence and offence. The architecture category aims to design and impose stricter security measures than equipment vendors have or to design more restrictive security policies than INFOSEC has. It encompasses all aspects of the designed safeguarding of cyberspace regarding vulnerabilities such as patching and updating. The passive defence category includes all the tools and systems needed to monitor networks and related systems or to provide security without human interaction, such as vulnerability scanning and penetration testing. The next phase is active defence, which encompasses activities of monitoring and analysing the threats and managing them or responding to them. These include deception, honey pots and threat hunting. The intelligence category is the product and process of collecting data, analysing them to obtain information on threats and potential adversaries and to produce a knowledge base. The last phase is the offence category and represents legal countermeasures or measures of self-defence of the entity outside its network such as the hack-back.[28]

[26] The ISO Platform, 2016, e-source; IT Governance Blog, 2018, e-source; Hooda, 2019, e-source, Klump, 2018, e-source.

[27] E.g. INFOSEC design and configure group policy of operational system, while CS is protecting the data, user and ICT against the breaches, intrusion, attack, etc., after the installation (City University by Seattle, 2019, e-source).

[28] Lee & Lee, 2016, pp. 4-5.

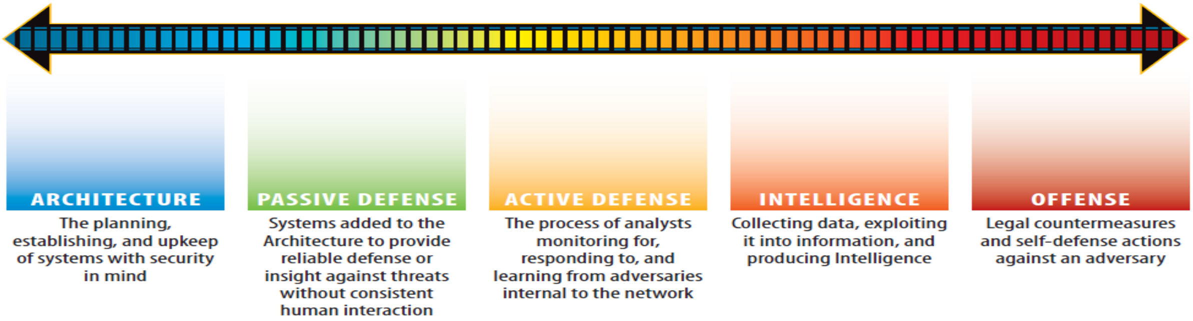

ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind
PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence
OFFENSE
Legal countermeasures and self-defense actions against an adversary

Figure 6: The Sliding Scale of CS[29]

The aim of this paper is not to determine if the INFOSEC concept is obsolete, but rather to make a delineation between the INFOSEC and CS concepts currently in place. Each deals with the protection and defence of information, data and systems, but we have found five main differences: any realm vs. cyber realm; any type of information vs. digital data; any system vs. ICS; all threats vs. cyber threats; and future risks vs. immediate risk and the ability to stop the current cyber threat. In any case, none of the concepts deals with ICT as a whole, but rather with IT and networks alone.

The sub-elements of Table 4 are based on the NIST CS framework[30] and the CS concepts of the entities. One of the 18 entities did not have an accepted definition, while NIST had four. Nine believed that the CIA triad should be involved, but did not define against what threats, which is per se self-evident, as we are cope with the cyber realm. They divided threats into cyber threats and cyber attacks, although the latest is the cyber threat per se already. The most commonly used activity is 'protection', but only two out of the 18 used this activity with a combination of 'defence' and four in combination with other actions. The words 'protect' and 'defence' can be understood differently depending on who is reading them: civilian, military or political.

Cyber security																		
	Activity								Threats			CIA triad					Measures	
	Identify	Protect	Preserv	Prevent	Defend	Detect	Respond	Recover	ND	CA	CT	C	I	A	Au	NR	Technical measures	Non-technical measures
UN	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
ISO	@	@	√	@	@	@	@	@	√			√	√	√	√	√	@	@
NIST 1	@	√	@	√	@	@	@	√	√			√	√	√	√	√	@	@
NIST 2	@	√		@	√	@	@			√							@	@
NIST 3	@	√		√	@	√	√			√								
NIST 4	@	@		√	@	@	@	√	√			√	√	√			@	@
EU	@	√	@	@	@	√	@			@	√	√	√	√	√	√	@	@
NATO	@	√		@	@	@	@		√			√	√	√	√	√	@	@
CCDCOE																		
Czech Republic	@	√		@	@	@	@		√								@	@
Estonia	@	√		@	@	@	@			@	√						@	@
Greece																		
Japan	@	@		√	@	@	@	@			@						@	@
Luxembourg	@	√		@	@	@	@		√			√	√	√	√	√	@	@
Portugal	@	√		@	@	@	@		√			√	√	√	√	√	@	@
Slovakia	@	@		@	@	@	@			@	@	√	√	√	√		@	@
State 1	@	√		@	@	@	@		√								@	@
State 2	@			@	@	@	@		√			√	√	√	√		@	@
State 3	@	√		@	√	@	@			√	√						@	@
State 4	@	√		@	@	@	@			√	@						@	@
United Kingdom	@	√		@	@	@	@				@						@	@

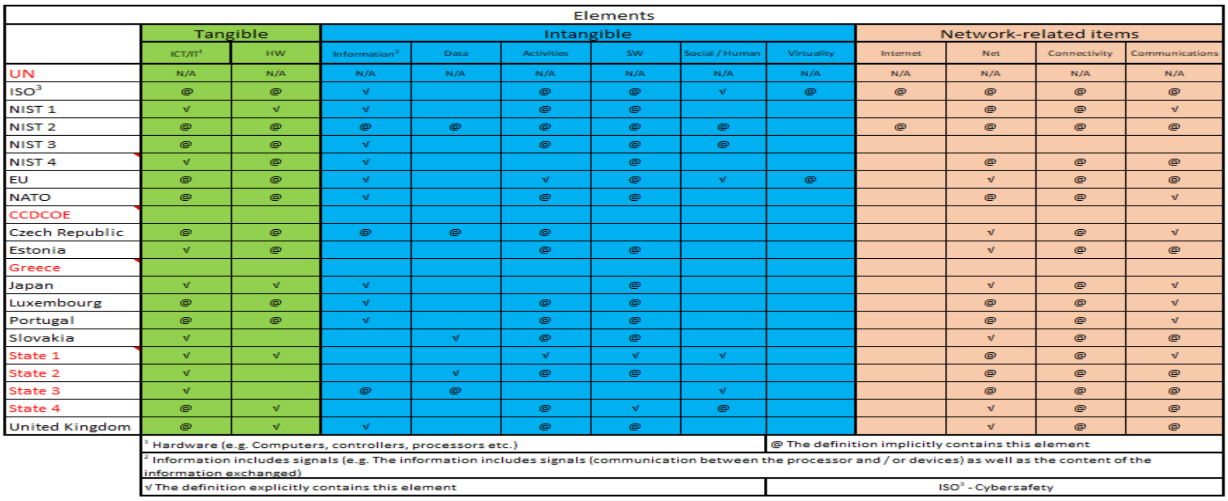
√ The definition explicitly contains this element	@ The definition implicitly contains this element
ND - Not Defined	CA - Cyber Attack; CT - Cyber threat
C - Confidentiality	ISO – ISO Cybersafety
A - Availability	Au - Authentication
I - Integrity	NR - Non-repudiation.

Table 4: Comparative analysis definition of the CS by taken Action

Table 5 draws the sub-elements which should be protected and the differences between entities' CS concepts. The main focus is on the protection of tangible and network-related element, while intangible elements are not so well included. The main shortcomings of the definitions regarding protection are the omission of sub-elements of the internet, software, the personal layer and virtual space as cyberspace is

[29] Lee, 2015, p. 2.
[30] NIST, 2018, p. 6.

multi-layered[31] and needs to be fully addressed. In addition, some entities define information protection instead of data protection as CS does not define the difference between data and information, but implements the protection of all critical ICS and data stored, processed and transmitted by ICS (Figure 1). The defining value data and critical systems is a task of IA.



	Elements											
	Tangible		Intangible						Network-related items			
	ICT/IT[1]	HW	Information[2]	Data	Activities	SW	Social / Human	Virtuality	Internet	Net	Connectivity	Communications
UN	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
ISO[3]	@	@	√		@	@	√	@	@	@	@	@
NIST 1	√	√	√		@	@				@	@	√
NIST 2	@	@	@	@	@	@	@		@	@	@	@
NIST 3	@	@	√		@	@	@					
NIST 4	√	@	√			@				@	@	@
EU	@	@	√		√	@	√	@		√	@	@
NATO	@	@	√		@	@				@	@	√
CCDCOE												
Czech Republic	@	@	@	@	@					√	@	√
Estonia	√	@			@	@				√	@	@
Greece												
Japan	√	√	√			@				√	@	√
Luxembourg	@	@	√		@	@				@	@	√
Portugal	@	@	√		@	@				@	@	√
Slovakia	√			√	@	@				√	@	@
State 1	√	√			√	√	√			@	@	√
State 2	√			√	@	@				@	@	@
State 3	√		@	@			√			@	@	@
State 4	@	√			@	√	@			√	@	@
United Kingdom	@	√	√		@	@				√	@	@

[1] Hardware (e.g. Computers, controllers, processors etc.)

@ The definition implicitly contains this element

[2] Information includes signals (e.g. The information includes signals (communication between the processor and / or devices) as well as the content of the information exchanged)

√ The definition explicitly contains this element

ISO[3] - Cybersafety

Table 5: Comparative analysis definition of the CS by Elements

An explicit and implicit understanding of the activities, threats and actions of CS entity concepts is shown in Table 4 and Chart 6. They show the sum of the implicitly and explicitly included elements and differences between the CS concepts of the entities in terms of their measures and activities, CIA triad and sources of threat. Most explicitly include 'protection' as the primary activity of safeguarding cyberspace or the CIA triad, while others prefer to use other words such as 'preserve' (the ISO) or 'prevent damage to' (NIST 4, Japan) or do not define the required action. Thus, based on the understanding and perception of the primary activity, it is left to the reader to choose which other activities are implicitly included and to provide the overall value of the individual concept. This again depends on the type of reader (civil, military or political) and on whether the reader is a native speaker or not. Consequently, the overall value of an individual concept does not necessarily coincide with the entity's evaluation. In addition, some entities do not address threats explicitly, while others divide threats into cyber threats and cyber attacks, although it is generally known that a cyber attack is one of the types of cyber threats. Such an approach only confuses the mutual understanding of the entities' concepts and in the defining activities that the CS concept is supposed to include.

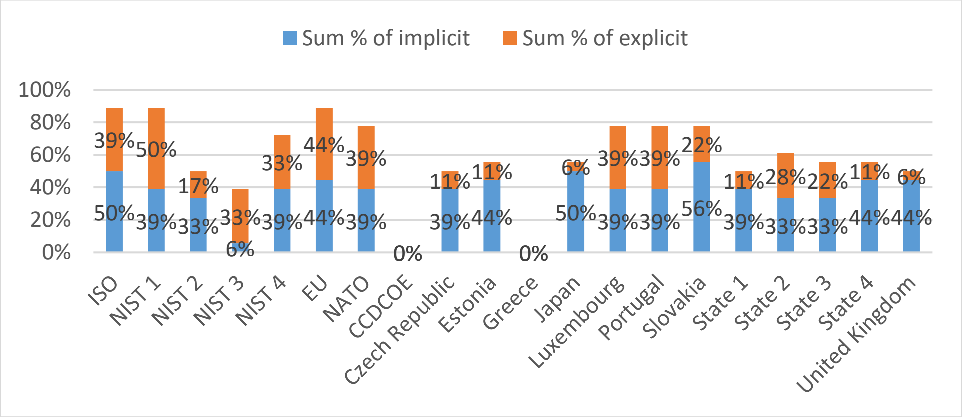


Chart 6: Explicitly and implicitly included elements in the definition of CS by Action

[31] Ministry of Defence Shrivenham, 2016, pp. 5-7; Clark, 2010, pp.1-2; JP 3-12, 2018, pp. I-2 – I-3.

In estimating the elements to be protected, we also used cyberspace entity definitions as some entities listed only cyberspace instead of directly defining the elements to be protected. Such an approach works if there is consistency and coherence between definitions, otherwise it causes ambiguity and confusion. Instead of ICS or ICT, the entities used different terms such as computer, hardware, software, electronic communication systems, electronic information and communication systems, electronic communications, other electronic systems, networks and IS which made it difficult to evaluate the sub-elements to be addressed in the CS concept (see Chart 7). Most of the sub-elements are marked as implicit and Chart 7 shows that most entities omit the sub-element of the social layer (human and virtual persona; cyber safety[32]) and the internet. Thus, it is left to the reader to decide what the CS concept means and how they evaluate it, which depends on having detailed knowledge of ICS and other cyber-related concepts, but the evaluation of the reader does not need to coincide with the evaluation of entity.

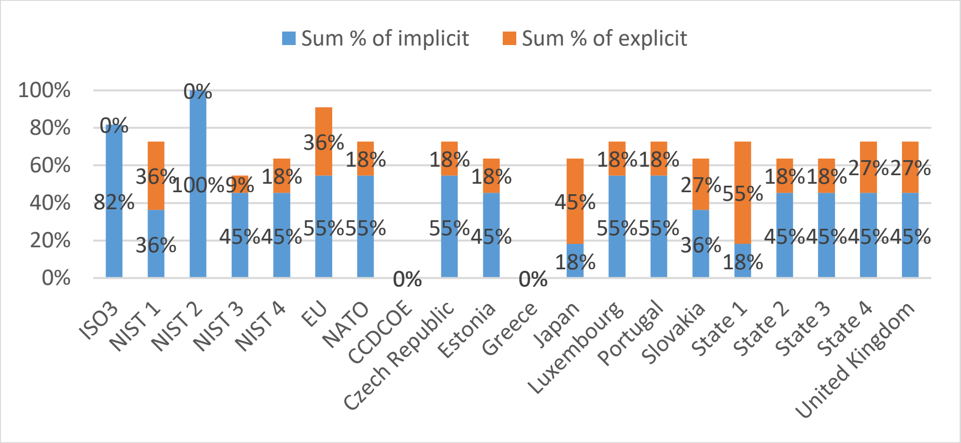
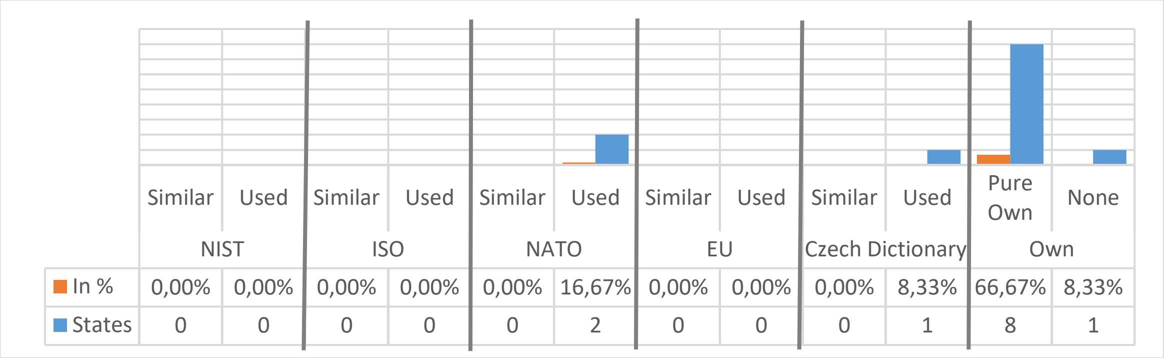


Chart 7: Explicitly and implicitly included elements in the definition of CS by Elements

The coherence of the definitions between the states and organisations is reflected in Chart 8. NATO's goal is to protect information and ICS, while the EU's goal is to protect cyberspace, its users and affected persons from cyber threats. Unlike organisations, some states seek to protect, secure and defend cyberspace, or protect ICS and some have no defined goals but define CS as a set of legal, organisational, technological and educational tools that can protect cyberspace. Only two states use the NATO definition verbatim (Luxembourg and Portugal), the Czech Republic uses its own, eight have their own understanding of the CS concept and one does not have a CS concept. The EU advocates the concept of CS as a superset of INFOSEC,[33] which is contrary to the generally accepted understanding of both concepts. There is thus no coherence between the definitions of states and organisations and no consistency as states do not pursue the concepts of organisations, which significantly affects the effectiveness of global CS.

[32] the ISO distinguishes CS from cyber safety: 'the condition of being protected in cyberspace' (the ISO/IEC 27032, First edition, 2012). Merriam-Webster dictionary defines cybersafety as 'safe practices when using the Internet to prevent personal attacks or criminal activity' (Merriam-Webster, Dictionary: cybersafety, 2021, e-source).

[33] Galinec, Možnik and Guberina are in favour of the EU approach, but they do not follow the holistic approach of INFOSEC, but focus exclusively on the CIS. (Galinec, Možnik, & Guberina 2017, pp. 273-274).



	NIST		ISO		NATO		EU		Czech Dictionary		Own	
	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Pure Own	None
🟧 In %	0,00%	0,00%	0,00%	0,00%	0,00%	16,67%	0,00%	0,00%	0,00%	8,33%	66,67%	8,33%
🟦 States	0	0	0	0	0	2	0	0	0	1	8	1

Chart 8: Similarity of 'CS' definitions according to organisations' dictionaries

3.1.4 Cyber defence

Cyber defence (CD) is yet another term that causes a lot of confusion and is vague compared to the INFOSEC and CS concepts. Our research has found that there is no uniform distinction between CS and CD [34]or between active and passive CD. Some experts argue that the only difference is whether the terminology is used in a civilian or military environment.[35] This is said to arise from legal and cultural understandings of the functions of the state in relation to citizens, with the state using defence (military forces) as a fundamental function of the state against external threats. Da Silva argues that the dilemma between CS and defence cannot exist as cyberspace is not a classic domain with clear state boundaries, so defence cannot be conducted only by military means but must include civilian ones.[36] 'Security' and 'defence' have different meanings, with 'security' meaning the state or quality of protection and protection against dangers or threats, while 'defence' means an act, action or ability to resist or defend against attack.[37]

NATO, the Open Technology Institute New America and Galinec et al. advocate that CD consists of proactive measures to detect and prevent cyber intrusion, attack and operation in a timely manner or proactive measures to respond to cyber threats to protect critical infrastructure, networks, entities and information.[38] Most authors argue that CD consists of both passive and active measures, hence it is also necessary to distinguish between passive and active cyber defence, with active defence also representing a grey zone of action (see Figure 7).[39] That grey zone is divided into light grey and dark grey, with active defence in the light grey on its own network and in the dark grey outside it, which can also be considered cyber offense.[40] The passive CDs are defence measures inside the defender's cyber infrastructure and without regular human intervention (the first line of defence), while active CD is proactive defence measures inside and outside the defender's cyber infrastructure. Yet, this describes a general approach but each state may interpret the terms used differently; for instance, under what circumstances and with what safeguards is the use of defence measures permitted in the dark grey zone or indeed when OC is allowed, and against what threats. Although beyond the scope of this study, these are important issues that need to be addressed by states and the international community.

[34] Klimburg, 2012, p. 9; Galinec, Možnik, & Guberina 2017, p. 273.
[35] Klimburg, 2012, pp. 12-13; Da Silva, 2016, pp. 1-2.
[36] Da Silva, 2016, pp. 1-2.
[37] Merriam-Webster, Dictionary: defensedefence, 2021, e-source.
[38] Štrucl, 2020, p.36.
[39] Denning, 2013, pp. 4-7; Lee, 2015, p. 1-2; Blair et al, 2016, p. 26; Lee & Lee, 2016, pp. 4-5; Barnes, 2018, pp. 1-2; Broeders, 2021, pp. 1-3.
[40] Broeders, 2021, p. 3.

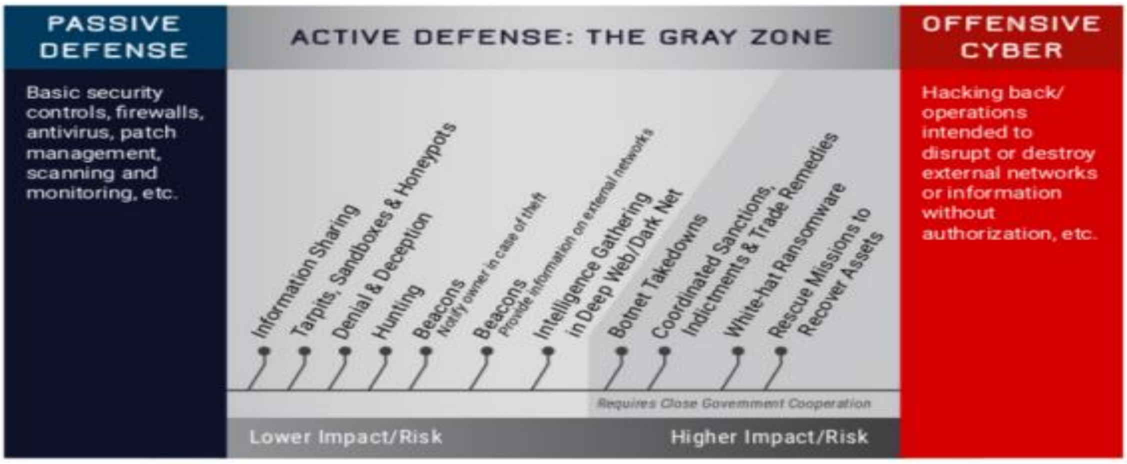
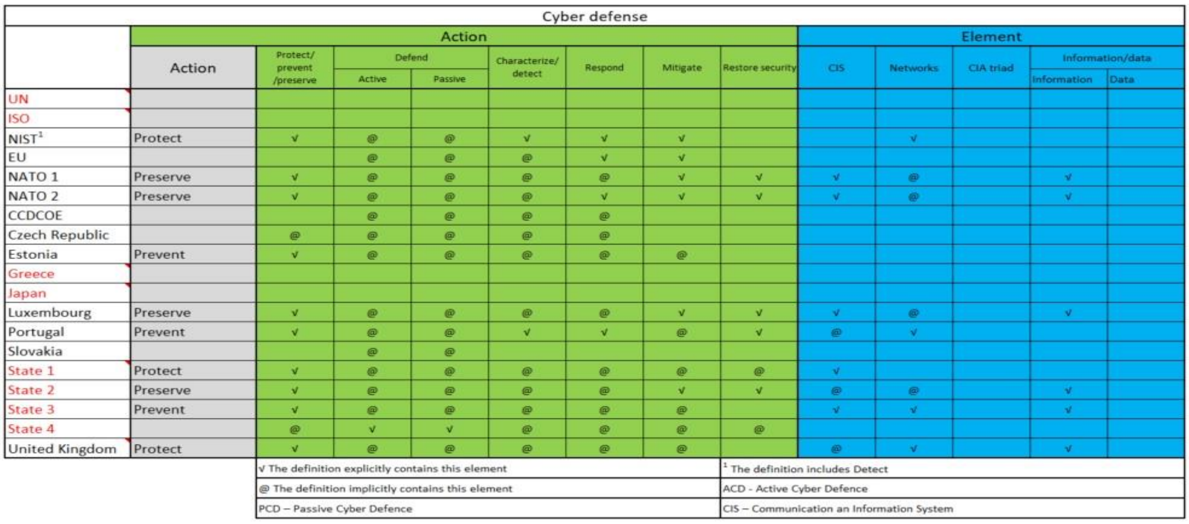

PASSIVE DEFENSE
Basic security controls, firewalls, antivirus, patch management, scanning and monitoring, etc.
ACTIVE DEFENSE: THE GRAY ZONE
Information Sharing
Tarpits, Sandboxes & Honeypots
Denial & Deception
Hunting
Beacons
Notify owner in case of theft
Beacons
Provide information on external networks
Intelligence Gathering in Deep Web/Dark Net
Botnet Takedowns
Coordinated Sanctions, Indictments & Trade Remedies
White-hat Ransomware
Rescue Missions to Recover Assets
Requires Close Government Cooperation
Lower Impact/Risk
Higher Impact/Risk
OFFENSIVE CYBER
Hacking back/ operations intended to disrupt or destroy external networks or information without authorization, etc.

Figure 7: Active Cyber Defence Measures[41]

Analysis of CD concepts shows that four of the 18 entities do not have accepted definitions and NATO has two (Table 6). To identify differences in the understanding of CD concepts between the addressed entities, the CD concept was divided into two main elements: actions within the IA concept and the elements to be protected. Table 6 shows that most entities include the necessary elements of 'action', but there is no consistency with the CS concept as less than 50% of the CD concepts discussed do not identify which elements need to be defended, including the CIA triad as the main element of CS. The entities have such approaches and there is no most common action identified. Some use the combination of the words 'prevent cyber attack and respond to it or deter them', while others have 'counter cyber threats to protect and preserve ICS.' The CCDCOE defines only 'active cyber defence', the Czech Republic distinguished CS from CD by the nature and intensity of the cyber attack, and the UK used the same definition as for CS. Thus there are many combinations of words that can be included in the definition of CD and this creates significant opacity when trying to define which actions can be included as part of CD, which is important as CD activities may constitute a violation of international law.



	Cyber defense												
	Action								Element				
	Action	Protect/ prevent /preserve	Defend		Characterize/ detect	Respond	Mitigate	Restore security	CIS	Networks	CIA triad	Information/data	
			Active	Passive								Information	Data
UN													
ISO													
NIST[1]	Protect	√	@	@	√	√	√			√			
EU			@	@	@	√	√						
NATO 1	Preserve	√	@	@	@	@	√	√	√	@		√	
NATO 2	Preserve	√	@	@	@	√	√	√	√	@		√	
CCDCOE			@	@	@	@							
Czech Republic		@	@	@	@	@							
Estonia	Prevent	√	@	@	@	@	@						
Greece													
Japan													
Luxembourg	Preserve	√	@	@	@	@	√	√	√	@		√	
Portugal	Prevent	√	@	@	√	√	@	√	@	√			
Slovakia			@	@									
State 1	Protect	√	@	@	@	@	@	@	√				
State 2	Preserve	√	@	@	@	@	√	√	@	@		√	
State 3	Prevent	√	@	@	@	@	@		√	√		√	
State 4		@	√	√	@	@	@	@					
United Kingdom	Protect	√	@	@	@	@	@		@	√		√	

√ The definition explicitly contains this element

@ The definition implicitly contains this element

PCD – Passive Cyber Defence

[1] The definition includes Detect

ACD - Active Cyber Defence

CIS – Communication an Information System

Table 6: Comparative analysis definition of the Cyber Defence

The overall value and individual evaluation of explicitly and implicitly included elements in entities' CD concepts are shown in Chart 9, but implicitly labelled sub-elements may vary from readers' points of view

[41] Blair et al, 2016, p. 26.

depending on whether the sub-element can be considered implicit or not. In general, very few elements are explicitly included in CD entity concepts, especially with respect to sub-elements related to defence and response, which is the basis of any defence. Only State 4 includes active and passive defence measures. The entities use two words to describe a defensive act: ‘response’ and ‘counter’.[42] While the latter is an act of opposition or contradiction to the cyber threat or attack, ‘response’[43] is the act of direct reply to such a threat or attack. The concept of a CD should have a very clear definition in relation to the actions involved as ambiguities increase the scope of activities in the dark grey zone. It is left to the reader to interpret which activities are included in the concept, depending on the type of reader (civil-military, political) and whether the reader is a native speaker or not.

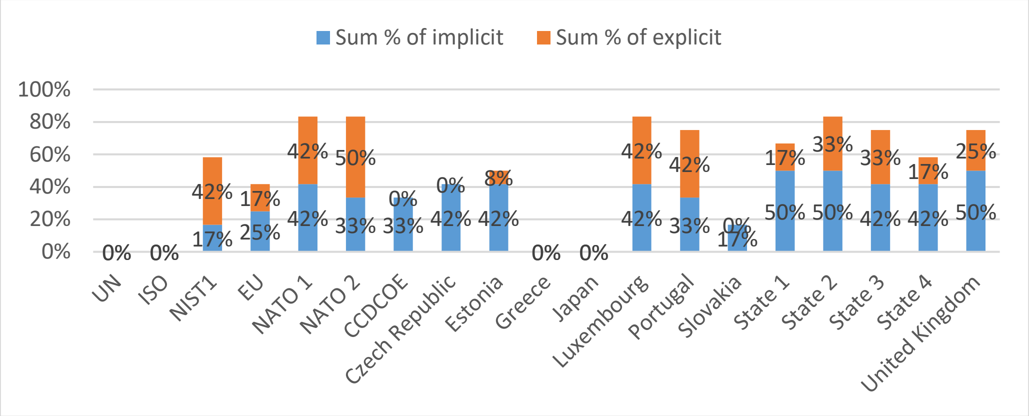
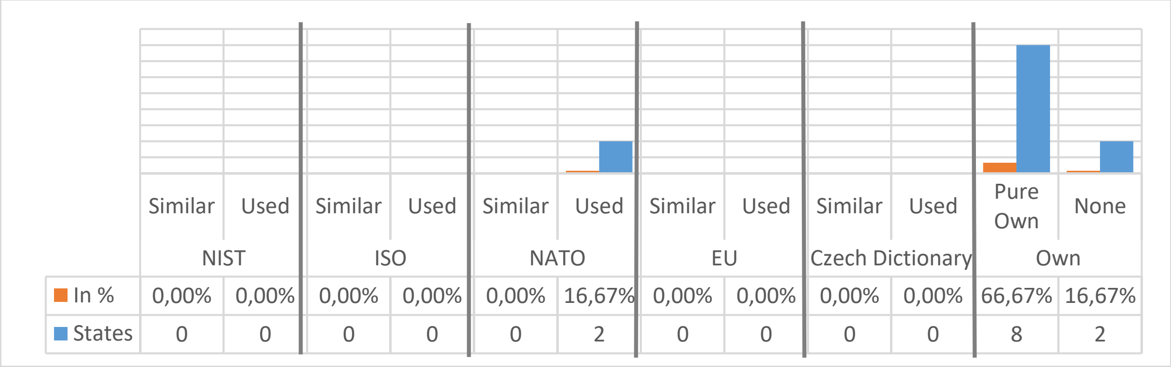


Chart 9: Explicit/ implicit included elements in the definition of Cyber Defence

Our analysis of the coherence of the definitions between the states and organisations surveyed is shown in Chart 10. Although most states are essentially concerned with ‘defence mechanisms or measures’, their goals, objectives and actions of cyber defence differ, with some states treating these measures and mechanisms as preventing and deterring (prevent and discourage) cyber attacks, preventing and repelling (reject) cyber attacks or ensuring the durability of the entities, while NATO’s goal is to counter cyber threats and mitigate their effects and the EU’s is to mitigate and respond. Based on their words, we estimated that no state has a similar definition to one of the reference organisations used in this study and that only two states use the NATO definition verbatim (Luxembourg and State 2), eight have their own understanding of the CS concept and two do not have a concept at all. Therefore, we can generally conclude that there is no coherence between the definitions of states and organisations or there is no consistency as states do not pursue the concepts of organisations, which would significantly affect the effectiveness of common CD.



	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Pure Own	None
	NIST		ISO		NATO		EU		Czech Dictionary		Own	
🟧 In %	0,00%	0,00%	0,00%	0,00%	0,00%	16,67%	0,00%	0,00%	0,00%	0,00%	66,67%	16,67%
🟦 States	0	0	0	0	0	2	0	0	0	0	8	2

Chart 10: Similarity of ‘CD’ definitions according to organisations’ dictionaries

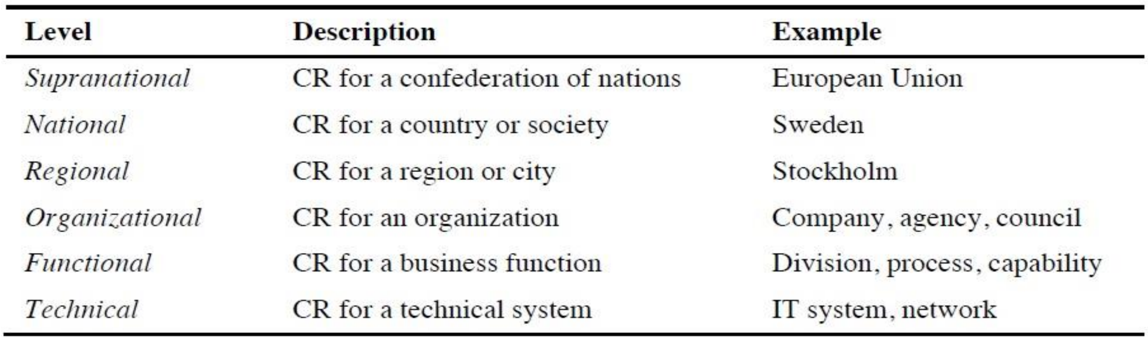
[42] Merriam-Webster, Dictionary: counter, 2021, e-source.

[43] Merriam-Webster, Dictionary: response, 2021, e-source.

3.1.5 Cyber resilience

Cyber resilience (CR) is another term in the cyber world which needs to be defined. Since the 2012 World Economic Forum meeting in Davos, the concept of CR has begun to gain importance and attention. Many authors argue that in the complex cyberspace and increasingly sophisticated threats and the internet of things (IoT), CS and CD are no longer sufficient. It is necessary to develop CR that allows the company to operate smoothly and deliver results regardless of the diversity and scale of cyber incidents.[44]

Kott and Linkov observe that the most widely used definition of CR is that of the National Academy of Sciences (NAS): 'the ability to prepare and plan for, absorb, recover from and more successfully adapt to adverse events'.[45] Björck et al define CR as the 'ability to continuously deliver the intended outcome despite adverse cyber events' and define the 'ability' as meaning to be able to continuously deliver (Including in the case of failure of regular delivery mechanisms) the intended outcome on different levels (Table 7): [46]



Level	Description	Example
Supranational	CR for a confederation of nations	European Union
National	CR for a country or society	Sweden
Regional	CR for a region or city	Stockholm
Organizational	CR for an organization	Company, agency, council
Functional	CR for a business function	Division, process, capability
Technical	CR for a technical system	IT system, network

Table 7: Cyber resilience considered at different levels[47]

CR is thus the ability of a system, organisation, mission or business process to anticipate, (plan to), withstand/resist/respond, absorb, adapt and recover from adversary events to ensure continuously deliver the intended outcome. Hence, CR is a combination of business continuity, INFOSEC, CS and CD as the organisation should evaluate all risks (including cyber incidents with the kinetic consequences), threats and vulnerabilities and should be prepared to encounter them when they occur.

An obvious issue arises in identifying the difference between CR and CS. There are many overlaps, but two major differences. CS focuses on preventing cyber threats from happening, while CR focuses on the assumption that an organisation will undoubtedly face a cyber threat, so it is necessary to plan the response and continued operation of the organisation when a cyber incident happens. Björck et al highlight five key differences in the characteristics of the two concepts, pointing out that the concept of CR must be built into the system and not added and the ICS architecture must be layered and allow for partial failure (Table 8). Therefore, CS protects ICS and valued data in general, while CR steps in when existing CS measures fail by hardening existing CD against cyber threats to ensure business continuity with no or minimal impact.

Aspect	CS	Cyber Resilience
Objective	Protect CIS	Ensure business delivery

[44] Björck et al, 2015, p. 311; Galinec & Steingartner, 2017, pp. 13-15; Kott & Linkov, 2019, pp. 1-3; Dupont, 2019, pp. 1-2; Hausken, 2020, pp. 1-3.

[45] Kott & Linkov, 2019, p. 30.

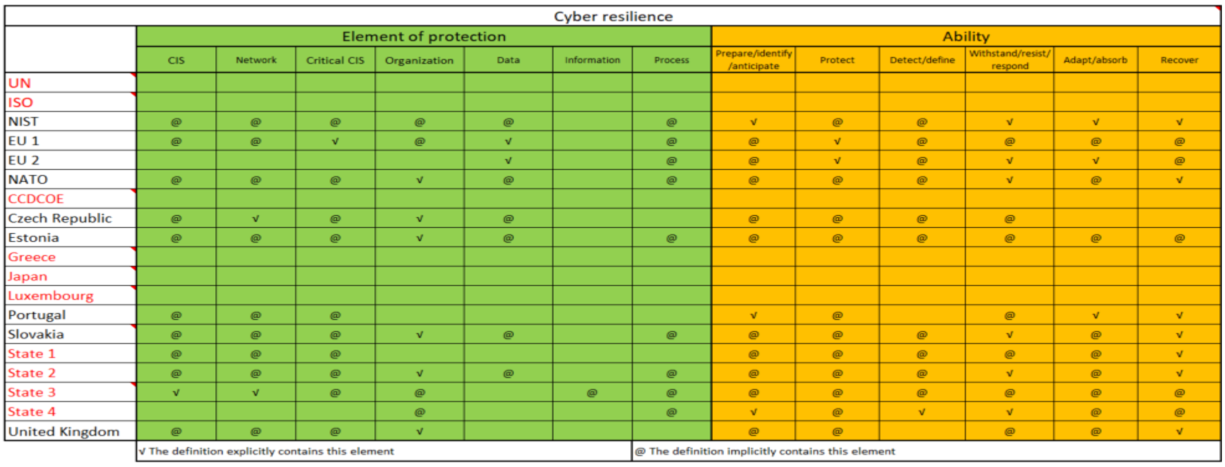
[46] Björck et al, 2015, p. 312.

[47] Ibid.

Intention	Fail-safe	Safe-to-fail
Approach	Apply security from the outside[48]	Build security from within
Architecture	Single layered protection[49]	Multi-layered protection
Scope	Atomistic, one organisation	Holistic, network of organisations

Table 8: Characteristics of CS vs. Cyber Resilience[50]

The analysis of the concept of CR is thus divided into the element 'an ability' and 'elements of (needed) protection'. As shown in Table 9, the six entities do not have a defined CR concept, while the EU has two. Despite the CR concept being based on the ability to cope with the cyber threats to deliver the intended outcome, some of the entities believe that information or data and processes are not elements to be addressed in the CR concept. There is thus no coherence and consistency with other cyber concepts as the main objectives of INFOSEC and CS are the protection of the CIS and information or valuable data. The only difference in the concepts are protection (CS) vs. defence (CD) vs. hardened protection and defence (CR). However, the elements of protection needed should be the same (including the CIA triad) to ensure business continuity.



	Cyber resilience												
	Element of protection							Ability					
	CIS	Network	Critical CIS	Organization	Data	Information	Process	Prepare/identify /anticipate	Protect	Detect/define	Withstand/resist/ respond	Adapt/absorb	Recover
UN													
ISO													
NIST	@	@	@	@	@		@	√	@	@	√	√	√
EU 1	@	@	√	@	√		@	@	√	@	@	@	@
EU 2					√		@	@	√	@	√	√	@
NATO	@	@	@	√	@		@	@	@	@	√	@	√
CCDCOE													
Czech Republic	@	√	@	√	@			@	@	@	@		
Estonia	@	@	@	√	@		@	@	@	@	@	@	@
Greece													
Japan													
Luxembourg													
Portugal	@	@	@					√	@		@	√	√
Slovakia	@	@	@	√	@		@	@	@	@	√	@	√
State 1	@	@	@					@	@	@	@	@	√
State 2	@	@	@	√	@		@	@	@	@	√	@	√
State 3	√	√	@	@		@	@	@	@	@	@	@	@
State 4				@			@	√	@	√	√	@	@
United Kingdom	@	@	@	√				@	@		@	@	√
	√ The definition explicitly contains this element						@ The definition implicitly contains this element						

Table 9: Comparative analysis definition of the Cyber Resilience

In estimating the elements visualised in Table 9, we also used other cyber-related definitions since some entities used an agnostic or an overly general approach. Such an approach per se is not an issue until there is consistency and coherence between all definitions, otherwise it causes ambiguity and confusion. Chart 11 reflects our understanding of what should be the implicitly included sub-elements, which does not necessarily coincide with the understanding of any other reader. It is not necessary for everyone to understand the words 'protect' or 'prevent' in the same way and which actions include these two terms or what the entities consider 'resist' or 'withstand' to mean. In addition, we do not know whether the entities in the 'system' also include data, information and processes or not. Chart 11 shows that the majority of entities do not explicitly include either the basic sub-elements of 'ability' or the basic elements of protection needed, while all other implicitly included sub-elements are a matter of our vocabulary and knowledge of

[48] CS is applied on a system, while cyber resilience is inner part of the system and the general operation of the business. (Björck et al, 2015, p. 314)
[49] With regard to CS, each layer of the inner structure of the system is designed to ensure the fail-safe of system layers and their relationships, while in cyber resilience, each layer must be designed to follow the principle safe-to-fail and is suitable for the restoration of each layer to provide business operations. (Ibid, p. 314)
[50] Ibid, pp. 313-314.

basic terminology (Appendix 1). Thus, the reader is left to understand the concept of CR and how to evaluate it, which depends on his professional function (civilian-politician-soldier), knowledge of ICS and understanding of grammar.

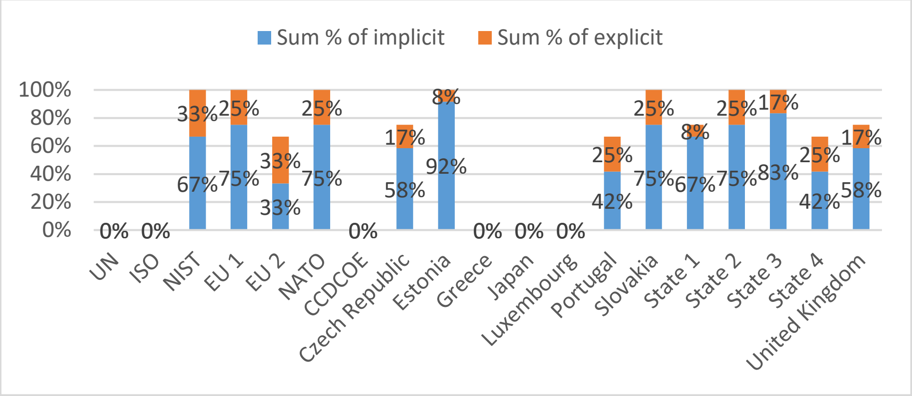
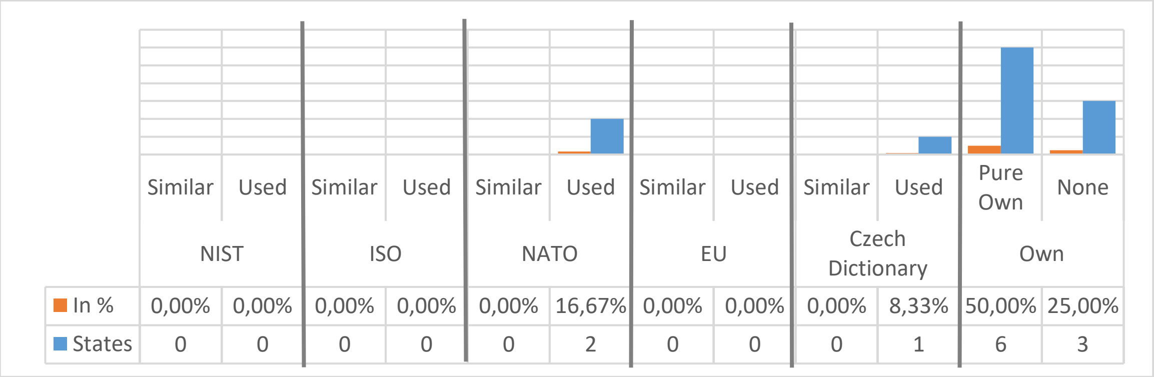


Chart 11: Explicit/ implicit included elements in the definition of Cyber Resilience

At first glance, there are no significant differences between states and organisations in terms of the purpose of the CR concept (Table 9) as all CR concepts are based on the ability to resist threats and to recover when they occur. However, a detailed analysis shows that there are differences in the approaches to implement CR concepts (Chart 12). The NATO concept is based on the overall technical and procedural ability of systems and organisations to withstand a cyber incident and recover from them, while the EU concept is based on the ability to protect electronic data and systems from cyber attacks and to resume business operations quickly or on the ability to prevent, resist, mitigate, absorb, accommodate to and recover from an incident. States define the CR concept as the ability of systems, organisations and platforms to resist and defend against the effect of outages; to maintain or restore CS; to tolerate, accept and recover; or as a state's, situation's or service's ability to provide their services. There is a difference in the choice of sources of threat that the entity should resist as NATO includes cyber incidents and the EU cyber attacks, while states have a wide range of sources of threats including cyber attacks, deliberate cyber attacks, cyber threats, natural threats or disasters or incidents due to malicious events. Slovakia has stated that it uses the definitions adopted in NATO and the EU, although the two differ in their approach. Based on the different approaches and words used of states and organisations, we estimated that no state has a similar definition to the organisations and that only two states use the NATO definition verbatim (Slovakia and State 2), the Czech Republic uses its own dictionary, six states have their own understanding of the CR concept and three states do not have a CR concept at all. Therefore, there is no coherence between the definitions of states and organisations or there is no consistency as states do not pursue the concepts of organisations, which significantly affects the effectiveness of the common approach to CR.



	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Pure Own	None
	NIST		ISO		NATO		EU		Czech Dictionary		Own	
🟧 In %	0,00%	0,00%	0,00%	0,00%	0,00%	16,67%	0,00%	0,00%	0,00%	8,33%	50,00%	25,00%
🟦 States	0	0	0	0	0	2	0	0	0	1	6	3

Chart 12: Similarity of 'CR' definitions according to organisations' dictionaries

3.1.6 Information environment

The information environment (IE) is not something new, but a term that is not often used. It exists in every community or organisation as the main goal is to connect individuals, information and processes according to their needs, interests or desires. The internet and modern technology have enabled organisations and interest groups to share information and data and connect processes and individuals within and outside a particular community in real-time. This is how many social networks have emerged, bringing individuals together according to their needs, goals or interests regardless of their geographical location.[51]

According to US Joint Publication 3-13 (JP 3-13), the IE is defined as 'the aggregate of individuals, organisations and systems that collect, process, disseminate or act on information' or 'three interrelated dimensions (physical, informational and cognitive) that continually interact with individuals, organisations and systems'.[52] Porche III took a different approach and defines IE as two partially intersecting areas where social networks are the webs of interaction and relationships among individuals, while cyberspace is the technical foundation on which the world relies to interact and exchange information.[53] Therefore, IE can be defined as the interconnected (three dimensions) functioning of ICS, individuals and organisations in which cyberspace enables their global interaction (Figure 8).

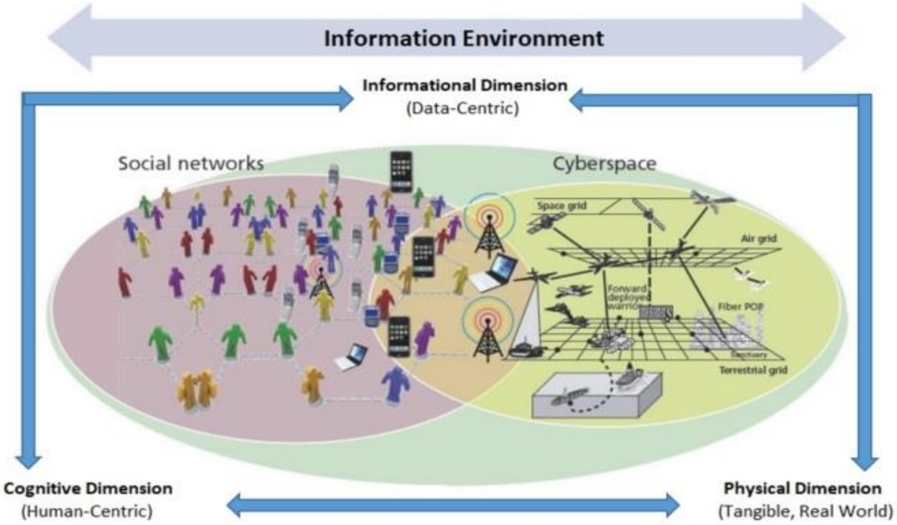


Figure 8: Information Environment[54]

The analysis of the IE concept is designed based on JP 3-13 and Porche III. As Table 10 shows, only eight of the 18 entities have a defined IE concept, representing 44.45% of respondents. All of these respondents include all three rudimentary sub-elements in their IE concepts: individual, ICS (including information) and organisation, while the cognitive dimension is omitted by three (Table 10). However, the cognitive domain is the one that separates cyberspace from the IE and at the same time creates various social networks and credible or false information. Therefore, the IE is significant for Strategic

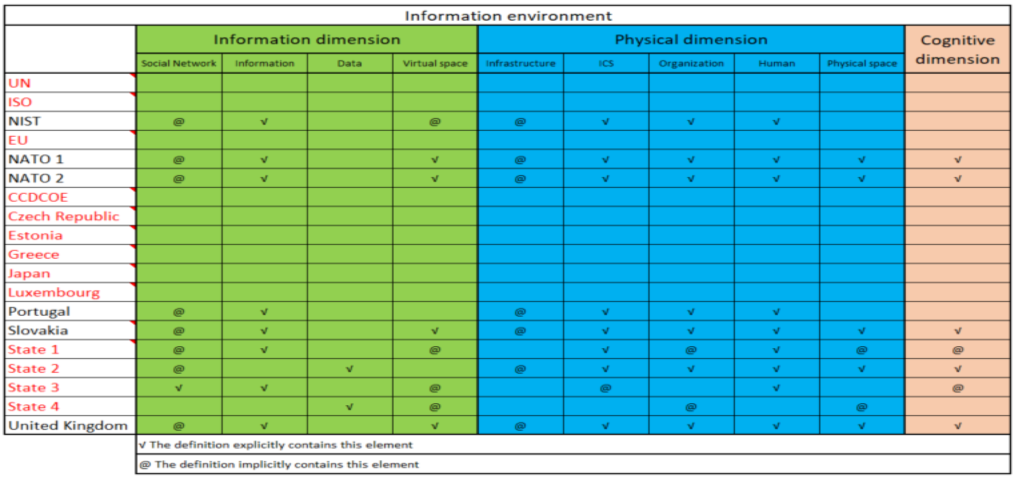
[51] Brikše, 2006, pp. 375-380.

[52] JP 3-13, 2014, p. IX. Physical Dimension: individuals, organisations, CIS, supporting infrastructure, books, newspapers or any other objects that are subject to empirical measurement; Information Dimension: the link between the physical and cognitive dimension, actions where information content and flow exist, and the medium by which information is collected, processed, stored, disseminated, and protected; Cognitive Dimension: the minds, perceptions and decisions of those who use information, or where individual and organisational consciousness exist. (Ibid, pp. I-2-I-3)

[53] Porche III, 2019, p. 2.

[54] Adopted from JP 3-13, 2014, p. I-2; Porche III, 2019, pp. 1-2.

Communications (StratComm) as it encompasses information, cyber and hybrid operations. IE and cyberspace are inextricably linked as social networks are a source of threats and at the same time subject to threats, therefore cyberspace should enable safe and secure IE.



	Information environment									
	Information dimension				Physical dimension					Cognitive dimension
	Social Network	Information	Data	Virtual space	Infrastructure	ICS	Organization	Human	Physical space	
UN										
ISO										
NIST	@	√		@	@	√	√	√		
EU										
NATO 1	@	√		√	@	√	√	√	√	√
NATO 2	@	√		√	@	√	√	√	√	√
CCDCOE										
Czech Republic										
Estonia										
Greece										
Japan										
Luxembourg										
Portugal	@	√			@	√	√	√		
Slovakia	@	√		√	@	√	√	√	√	√
State 1	@	√		@		√	@	√	@	@
State 2	@		√		@	√	√	√	√	√
State 3	√	√		@		@		√		@
State 4			√	@			@		@	
United Kingdom	@	√		√	@	√	√	√	√	√
	√ The definition explicitly contains this element									
	@ The definition implicitly contains this element									

Table 10: Comparative analysis definition of the Information Environment

Although the number of implicitly and explicitly included sub-elements differs, Table 10 shows that the definitions of entities do not differ significantly in general. The biggest deviation is in the sub-elements Social Network, Virtual Space and Infrastructure as only one respondent explicitly includes social networks, four Virtual space and none includes physical infrastructure (Chart 13). Although the Social Network is not explicitly included in most responses, we believe that the cognitive dimension should also implicitly include a Social Network as the minds of individuals or organisations influence social networking. However, there is a dilemma as to whether IE involves information or data. Social networks create false and unverified information from data, so we believe that data should be used instead of an element of information. In the end, we can conclude that the dilemma between the implicit and the explicit only exists in the sub-elements Social Network, Cognitive Dimension and Virtual Space and it is left to the reader to understand which sub-elements apply to them.

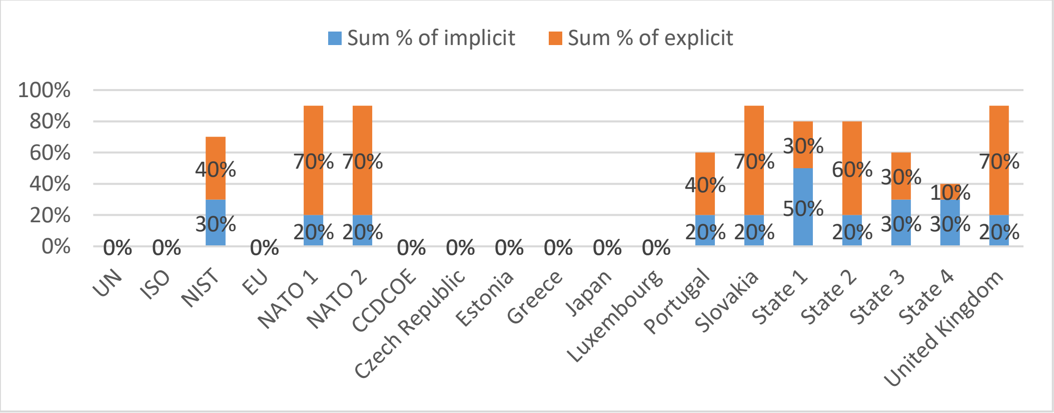


Chart 13: Explicit/ implicit included elements in the definition of the information environment

The analysis of the coherence of IE concepts considers the conceptual design of IE concepts based on the sub-elements of all three dimensions of IE (Chart 14). In its concept, NATO encompasses the cognitive, virtual and physical dimensions of information, individuals, organisations and systems. This concept is followed by Slovakia and the UK, while Portugal has a similar concept to NIST which does not consider these dimensions. Four entities have their own definitions that define IE as a cluster of social networks and cyberspace; or any environment that stores, processes and transmits data; or people and automated systems; or numerous social, cultural, cognitive, technical and physical attributes that impact on an individual, group, system, community or organisation; or any environment that stores, processes and transmits data. Therefore, we can conclude that there is no coherence between the definitions of states and organisations or there is no consistency as states do not pursue the concepts of NATO, which significantly affects the effectiveness of common the common approach to StratComm and consequently to information, hybrid and cyber operations.

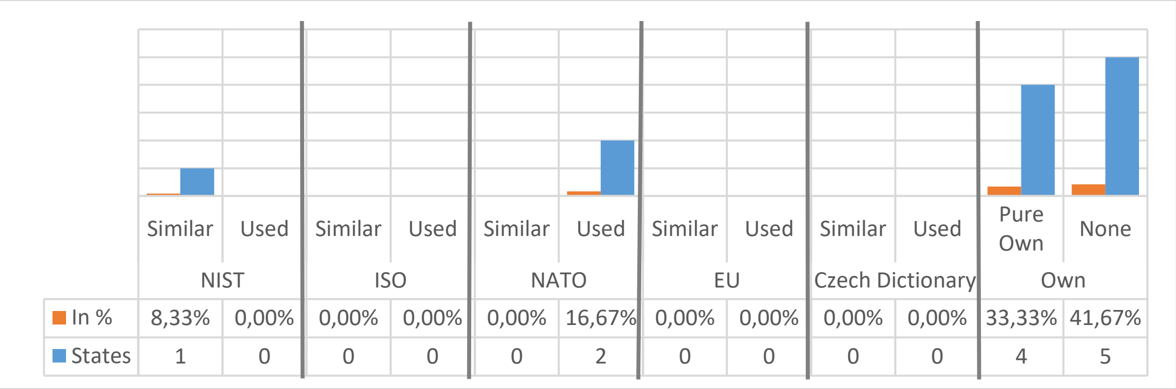


Chart 14: Similarity of 'IE' definitions according to organisations' dictionaries

3.1.7 Cyberspace

The term 'cyberspace' has not yet received a globally accepted definition, but most experts share a common concept: it is a collection of computer devices to store and use electronic information over networks and the internet.[55] Mbanaso and Dandaura note that cyberspace is sometimes tantamount to the notion of the internet or the view of a digital virtual realm as many definitions encapsulate the combination of the ICT and internet that enable the storage, processing, use and conveyance of information.[56] Ottis and Lorents found that many definitions of cyberspace have evolved, with many omitting key components of cyberspace such as human users and interactions between elements of cyberspace due to its dynamic nature.[57]

Clark and Probert follow the cyberspace concept defined by the US General Staff, with cyberspace divided into three layers (Figure 9). A layered approach is followed by the UK, however, it divides cyberspace into six layers.[58] The physical layer (UK – real layer) of cyberspace forms the foundation of a layered approach as consists of the physical location of ICT components (infrastructure - geographic components) and physical ICT components (tangible components – hardware, devices, wires) that support the logical layer (intangible and network-related components). The latter is based on logical programme code and represents an abstracted physical component to support the platform of cyberspace, consisting of the logical components of the network (UK – network layer) and data (UK – information layer), which

[55] Ottis & Lorents, 2010, p. 267; Clark, 2010, p. 1. Cyberspace: *'the online world of computer networks and especially the Internet'* (Merriam-Webster, Dictionary: cyberspace, 2021, e-source).

[56] Mbanaso & Dandaura, 2015, p. 18. U.S. Department of Defence: cyberspace is 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and and embedded processors and controllers'. The Russian-American CS Summit: cyberspace is 'an electronic medium through which information is created, transmitted, received, stored, processed, and and deleted'. (Ibid.)

[57] Ottis & Lorents, 2010, pp. 267-268. Ottis & Lorents proposed definition: 'Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems'. (Ibid, p. 268)

[58] Ministry of Defence Shrivenham, 2016, pp. 5-7; Clark, 2010, pp.1-2; JP 3-12, 2018, pp. I-2 – I-3. Logical layer is fundamental for information assurance processes and it can be often target for signals intelligence and cyber intelligence, surveillance and reconnaissance. (Ministry of Defence Shrivenham, 2016, p. 7)

comprises links and nodes, including data, applications and network processes. The last layer is the social layer which is created by abstracting data from the logical layer, obeying or ignoring certain rules (e.g. user authentication, unauthorised intrusions into the logical layer, etc.). The social layer thus represents the interaction (networking) of actual or virtual persons / entities (e.g. user account, e-mail and IP addresses, etc. UK – persona layer) in the logical layer and so form the character of cyberspace.[59]

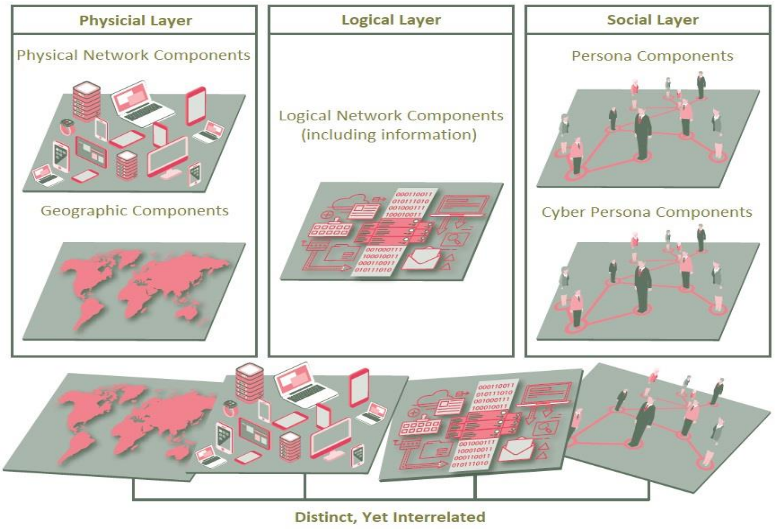
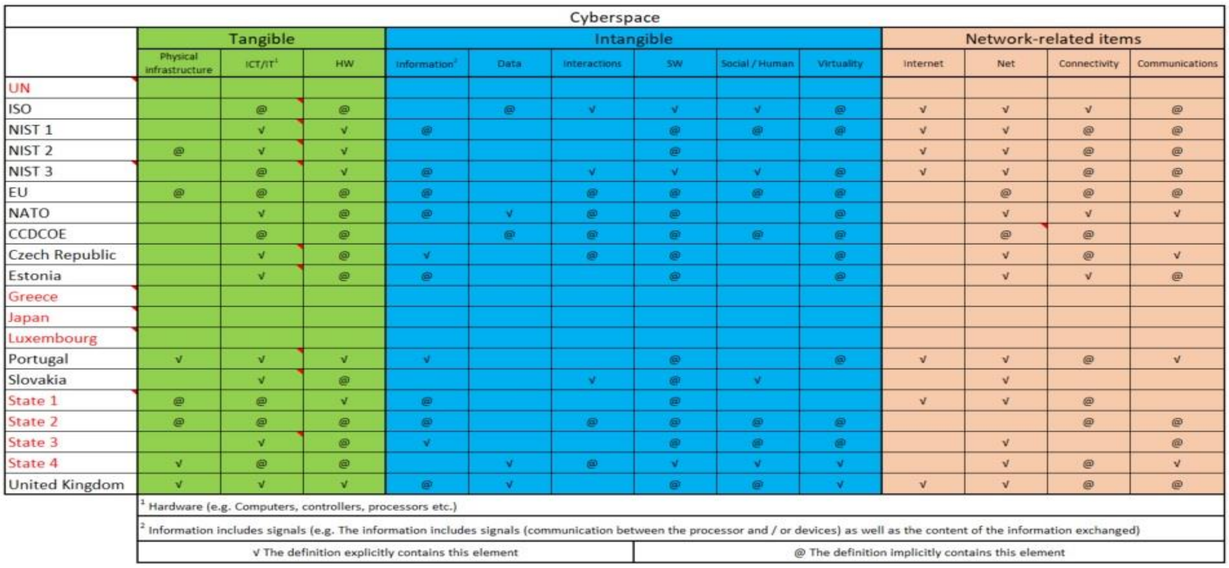

Physicial Layer
Physical Network Components
Geographic Components
Logical Layer
Logical Network Components (including information)
Social Layer
Persona Components
Cyber Persona Components
Distinct, Yet Interrelated

Figure 9: Cyberspace Layers[60]

Table 11 is divided into three basic elements – tangible, intangible and network-related items – which include all sub-elements of these layers. Five of the 18 entities do not have an accepted cyberspace definition, while NIST has three. We confirm the findings of Ottis and Lorents that some of the definitions omit key components such as users and interactions and also found that most respondents omit the sub-element infrastructure and the internet. Our next finding refers to information or data, where we can find a parallel with the concept of IE; in the narrow notion of cyberspace, we can agree that considering the sub-element ‘information’ is sufficient, but if we add the sub-element ‘internet’ or defining cyberspace as a ‘global domain’, then we should use the sub-element ‘data’, because the latter is the underpinning element to distinguish verified and unverified information. This concept is also followed by NATO, State 2 and the UK which include sub-element data in the information layer.

[59] Ministry of Defence Shrivenham, 2016, pp. 5.

[60] Adapted from: Clark, 2010, pp.1-2; JP 3-12, 2018, pp. I-3; Probert, 2019, p. 69.



	Cyberspace												
	Tangible			Intangible						Network-related items			
	Physical infrastructure	ICT/IT[1]	HW	Information[2]	Data	Interactions	SW	Social / Human	Virtuality	Internet	Net	Connectivity	Communications
UN													
ISO		@	@		@	√	√	√	@	√	√	√	@
NIST 1		√	√	@			@	@	@	√	√	@	@
NIST 2	@	√	√				@			√	√	@	@
NIST 3		@	√	@		√	√	√	@	√	√	@	@
EU	@	@	@	@		@	@	@	@		@	@	@
NATO		√	@	@	√	@	@		@		√	√	√
CCDCOE		@	@		@	@	@	@	@		@	@	
Czech Republic		√	@	√		@	@		@		√	@	√
Estonia		√	@	@			@		@		√	√	@
Greece													
Japan													
Luxembourg													
Portugal	√	√	√	√			@		@	√	√	@	√
Slovakia		√	@			√	@	√			√		
State 1	@	@	√	@			@			√	√	@	
State 2	@	@	@	@		@	@	@	@			@	@
State 3		√	@	√			@	@	@		√		@
State 4	√	@	@		√	@	√	√	√		√	@	√
United Kingdom	√	√	√	@	√		@	@	√	√	√	@	@

[1] Hardware (e.g. Computers, controllers, processors etc.)

[2] Information includes signals (e.g. The information includes signals (communication between the processor and / or devices) as well as the content of the information exchanged)

√ The definition explicitly contains this element

@ The definition implicitly contains this element

Table 11: Comparative analysis definition of cyberspace

The fragmented approach of the entities to define sub-elements (computer system, telecommunication networks, hardware, information technology) is reflected in Table 11 and the results in Chart 15. The analysis of entities' terminology is based on Appendix 1, which defines rudimentary terminology. Chart 15 reflects our view and understanding of the rudimentary terminology or which sub-elements are implicitly included, which does not necessarily coincide with the interpretation of any other reader and does not mean that the definition is bad. Everyone does not need to have the same understanding of a 'computer system' or a 'telecommunications network' and what elements these systems include. We cannot know exactly whether the entities in the 'system' also include data, information, people, software and interactions as the entities do not use uniform terms as CIS or ICT is. Nevertheless, we assessed that all entities explicitly or implicitly include all the basic elements of ICT, however, this evaluation represents our view and understanding of the basic terminology according to Appendix 1.

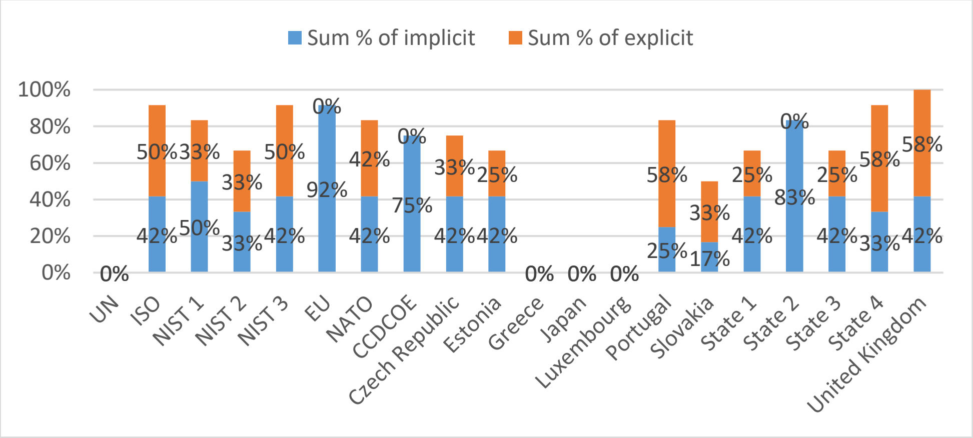
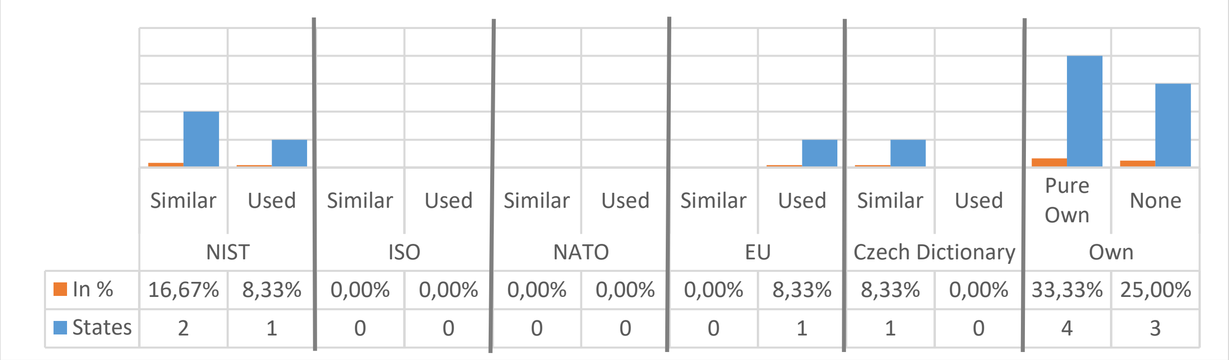


Chart 15: Explicit/ implicit included elements in the definition of cyberspace

The entities in question define and describe cyberspace in different ways, but all have in common that it is explicitly or implicitly composed of information and electronic technology or systems. A detailed analysis showed that we have four groups of entities, namely those that follow the NIST approach, Ottis and Lorent, a stand-alone approach and those that have not yet defined cyberspace (Chart 16). Thus, NATO, Portugal, the UK and State 1 (the latter uses the NIST definition verbatim) define cyberspace, similar to

NIST as a global domain consisting of all interconnected ICT and other electronic systems, networks and data, while the EU, CCDCOE and State 2 (the latter uses EU definition verbatim) use the Ottis and Lorents approach as a time-dependent set of tangible and intangible assets and electronic information. The Czech Republic defines cyberspace according to the Czech dictionary as a digital environment, while other states have defined it as a global environment, a global environment within the IE, an operational environment, a digital environment or a set of physical-digital infrastructures, networks and the electromagnetic spectrum. There are also differences in the cyberspace concept, with entities defining cyberspace as a global domain and others as a global information or digital environment or system. Thus, we can conclude that states do not follow the NATO or EU concepts which are inconsistent and that this also affects the effective implementation of the common security and defence policy of both organisations and the development of international rules on cyberspace.



	NIST		ISO		NATO		EU		Czech Dictionary		Own	
	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Pure Own	None
🟧 In %	16,67%	8,33%	0,00%	0,00%	0,00%	0,00%	0,00%	8,33%	8,33%	0,00%	33,33%	25,00%
🟦 States	2	1	0	0	0	0	0	1	1	0	4	3

Chart 16: Similarity of 'cyberspace' definitions according to organisations' dictionaries

3.1.8 Cyber attack

Cyber attacks are regular headline topics among politicians and journalists and there is usually no distinction made between a cyber attack and cyber espionage. A cyber attack is one of the cyber threats with the offensive objective to harm or damage, while cyber espionage or cyber exploitation is the cyber threat to steal classified or sensitive data or intellectual property. Cyber espionage is a form of cyber attack[61] as obtaining data often requires the penetration of an ICS. However, cyber espionage per se does not constitute a violation of customary international law and does not violate the rule of sovereignty or illicit intervention, yet it can violate national legislation, especially regarding intellectual property.

The rudimentary distinction between a cyber attack[62] and cyber espionage is technical in nature: a cyber attack's payload is destructive, while a cyber espionage payload is non-destructive as its goal is to obtain data. The cyber attack's primary goals are to harm and damage an entity's assets by altering, disrupting, degrading or destroying them. Cyber espionage is usually covert without harming ICS as it does not want to be detected.[63] Hence, different types and objectives of the cyber attack define the category of cyber threat or what constitutes different cyber-related actions/ breaches:

- cybercrime (illegal activity such as fraud, theft/piracy or paedophilia in or via cyberspace to gain financial or personal benefits);
- cyber terrorism (unlawful and violent attacks and threats in or via cyberspace to achieve political, social or ideological goals);

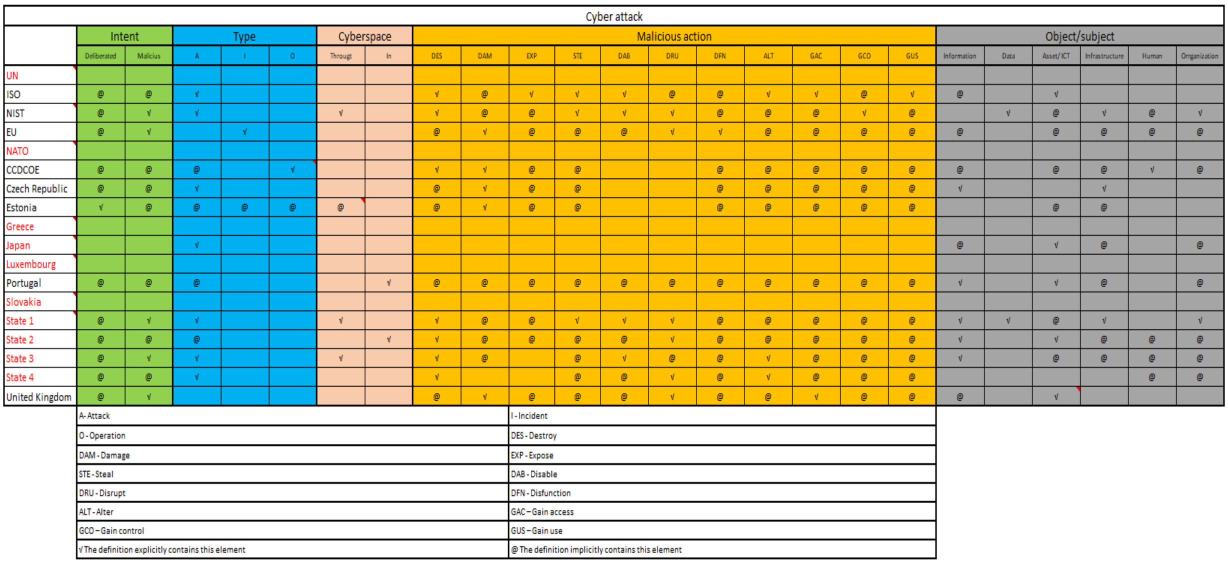
[61] Bendovschi, 2015, p. 26. Bendovschi splits different attack types into four categories, depending on the objectives of it: cyber-crime, cyber espionage, cyber war and hacktivism. (Ibid.)

[62] Merriam - Webster Dictionary: 'an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm' (Merriam - Webster Dictionary, cyberattack, 2021, e-source). Cambridge Dictionary: 'an illegal attempt to harm someone's computer system or the information on it, using the internet' (Cambridge Dictionary, cyberattack, 2021, e-source).

[63] Lin, 2010, pp. 63-64; Sander, 2019, pp. 365-367.

- cyber espionage[64] (stealing classified, sensitive data or intellectual property to gain information advantage or financial benefits in or via cyberspace);
- (offensive or defensive) cyber operation (politically motivated attacks as cyber espionage, cyber sabotage, cyber subversion, cyber manipulation, ransomware and military cyber attack to threaten national security and show cyber power).[65]

Although a cyber attack may be politically motivated and may constitute a violation of international law or lead to its violation, the UN and NATO have not yet defined the term, nor have Greece, Japan, Luxembourg or Slovakia, while Portugal and State 2 have similar definitions. Table 12 shows that most entities agree that a cyber attack is an attack, while the EU and Slovakia define it as a cyber incident and CCDCOE as a cyber operation expected to cause injury, death or damage or destruction of objects). All explicitly or implicitly see a cyber attack as an intentional or malicious act with the intent to cause harm or damage to ICS and information, with the Czech Republic emphasising that cyber attack is most commonly used politically or militarily motivated attack. The biggest discrepancy is in the sub-element ‘cyberspace’, ‘human’ and ‘information’ or ‘data’ as most entities do not consider cyberspace as a medium or environment for cyber attack and do not consider people as a potential target for attack or there is a lack of consistency with previously discussed concepts. According to some researchers and our understanding, the concept of CS deals with the protection of all digital data that underpin critical information.[66]



	Cyber attack																							
	Intent		Type			Cyberspace		Malicious action											Object/subject					
	Deliberated	Malicius	A	I	O	Througt	In	DES	DAM	EXP	STE	DAB	DRU	DFN	ALT	GAC	GCO	GUS	Information	Data	Asset/ ICT	Infrastructure	Human	Orrganization
UN																								
ISO	@	@	√					√	@	√	√	√	@	@	√	√	@	√	@		√			
NIST	@	√	√			√		√	@	@	√	√	√	@	@	@	√	@		√	@	√	@	√
EU	@	√		√				@	√	@	@	@	√	√	@	@	@	@	@		@	@	@	@
NATO																								
CCDCOE	@	@	@		√			√	√	@	@			@	@	@	@	@	@		@	@	√	@
Czech Republic	@	@	√					@	√	@	@			@	@	@	@	@	√			√		
Estonia	√	@	@	@	@	@		@	√	@	@			@	@	@	@	@			@	@		
Greece																								
Japan			√																@		√	@		@
Luxembourg																								
Portugal	@	@	@				√	@	@	@	@	@	@	@	@	@	@	@	√		√	@		@
Slovakia																								
State 1	@	√	√			√		√	@	@	√	√	√	@	@	@	@	@	√	√	@	√		√
State 2	@	@	@				√	√	@	@	@	@	√	@	@	@	@	@	√		√	@	@	@
State 3	@	√	√			√		√	@		@	√	@	@	√	@	@	@	√		@	@	@	@
State 4	@	@	√					√			@	@	√	@	√	@	@	@					@	@
United Kingdom	@	√						@	√	@	@	@	√	@	@	√	@	@	@		√			

A- Attack	I - Incident
O - Operation	DES - Destroy
DAM - Damage	EXP - Expose
STE - Steal	DAB - Disable
DRU - Disrupt	DFN - Disfunction
ALT - Alter	GAC – Gain access
GCO – Gain control	GUS – Gain use
√ The definition explicitly contains this element	@ The definition implicitly contains this element

Table 12: Comparative analysis definition of the Cyber Attack

Table 12 shows the diversity of entities’ approaches to defining the cyber attack concept in which concepts, sub-elements are marked explicitly or implicitly and our understanding of an individual sub-element does not necessarily coincide with the understanding of other readers or the author of the concept. Summarising the findings, states define cyber attack as an attack, electronic attack, act or action through a network or cyberspace or initiated in it, to cause harm to ICS and information or maliciously destroy disrupt, disable, change, collect, control, exploit, expose or obstruct a computing environment, infrastructure, computer system, networks, devices, essential information, integrity of data, entities of cyberspace or obtaining sensitive or strategically important information. However, neither the state nor

[64] Cyber espionage can be government or company sponsored, therefore can be divided on political, intelligence, military, industrial and economic espionage.
[65] Rid, 2013, p. XIV; Healey, 2019, p. 5; Osawa in Rõigas & Jermalavičius, 2021, pp. 2-3.
[66] Cthe ISO Platform, 2016, e-source; IT Governance Blog, 2018, e-source; Hooda, 2019, e-source, Klump, 2018, e-source.

the organisation explicitly lists all the malicious acts and targeted objects so we used the Merriam-Webster Dictionary to identify which sub-elements are also implicitly included. For example, the word 'damage' is defined as 'loss or harm resulting from injury to person, property or reputation',[67] therefore we evaluated that destruction, exposure, steal, disfunction and alteration should be implicitly included (Chart 17). However, to alter, expose or steal data, the perpetrator must gain access, control and use, so those malicious actions are also implicitly included. This is just one example of how difficult it is to clearly define the entities' cyber attack concepts, since 'disrupt' and 'disable' could also be implicitly included as those malicious actions could damage the reputation of an individual entity. Therefore, it is left to the reader to understand the concept of cyber attack, which is difficult if the definition includes too many potential sub-elements within its definition.

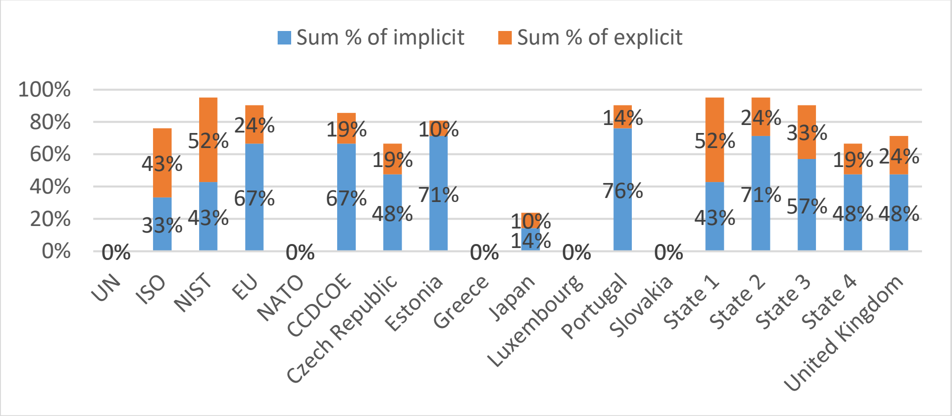
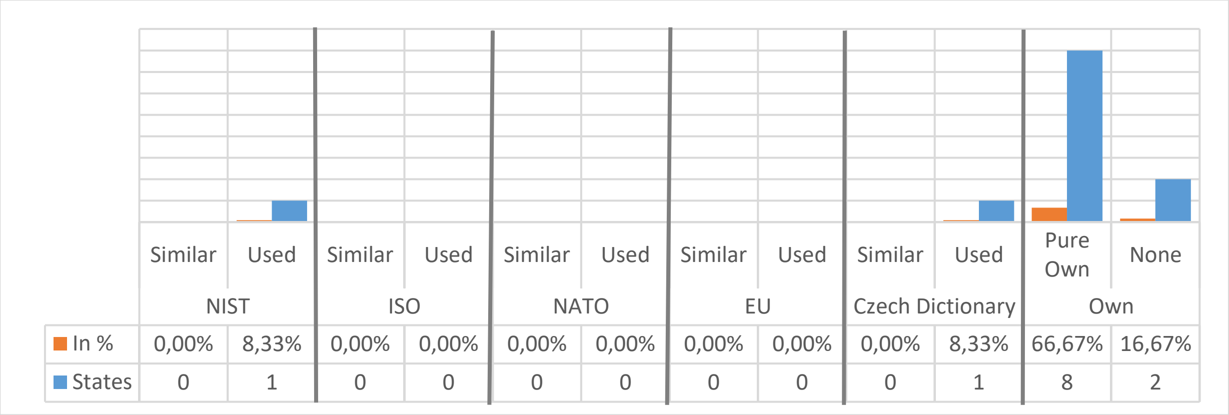


Chart 17: Explicit/ implicit included elements in the definition of Cyber Attack

Chart 18 shows the coherence of state, NATO and EU definitions of cyber attack. States use different words to define cyber attack as a deliberate or malicious act or action or incident or attack, with the aim to damage and harm the IT infrastructure or ICS and information or cyberspace by using either cyber tools or cyber means or network and IS or cyberspace. NATO[68] has not yet officially defined a cyber attack, while the EU defines it as any cyber incident triggered by malicious intent to damage, disrupt or make dysfunctional. Despite the entities' approach and words used, we estimated that no state has a similar definition to any organisation, that only State 1 used the NIST definition verbatim, that the Czech Republic uses its own dictionary, that eight states have their own understanding of a cyber attack and that two states do not have any definition. Consequently, our general finding is that there is no common understanding of what cyber attack is or should be and at the same time states do not pursue the concepts of organisations, which significantly affects a common international recognition of violations of international law and effective common defence against cyber attack under international law.

[67] Merriam-Webster, Dictionary: damage, 2021, e-source.

[68] CCDCOE defines CA as a 'cyber operation (offensive or defensive), that is reasonably expected to cause injury or death to persons or damage or destruction to objects'. (Tallinn manual 2.0 on the international law applicable to cyber operations, 2017, p. 564.)



	NIST		ISO		NATO		EU		Czech Dictionary		Own	
	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Pure Own	None
🟧 In %	0,00%	8,33%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	8,33%	66,67%	16,67%
🟦 States	0	1	0	0	0	0	0	0	0	1	8	2

Chart 18: Similarity of ‘cyber attack’ definitions according to organisations’ dictionaries

3.1.9 Cyber incident

The term ‘cyber incident’ (CI) is very rarely used in public and political debates and in addition to the abundance of other terminology, it causes additional ambiguities and vagueness in the national and international environment. For this study, we searched for professional literature but found that there was no common understanding of what a CI is.[69] However, the term is established, so it is necessary to understand the difference between a CI, a cyber event and a cyber attack.

All three terms describe activity regarding CIS, information and cyberspace, but because of the similarity are often confused. In general, a cyber event[70] is something that happens while CI[71] and cyber attacks are confirmed adverse events. Therefore, every CI or cyber attack can be an event, but not every event can be a CI or a cyber attack. To illustrate the rationale difference between cyber event and CI, we can use a malicious code attack: event – the user reports a potential malicious attack (virus); incident – the ICS exhibits behaviours typical of such an attack (virus).[72]

The (Abstract) Computer Emergency Response Team (CERT) taxonomy in Figure 10 distinguishes between a cyber event, a cyber attack and a CI. An event is when an action occurs on a specific target and poses a potential threat to an organisation. Taking into account the analysis of the event, the vulnerability, the tools used and the unauthorised consequences, we can determine whether it is a cyber attack or just a cyber event. Once a cyber attack is identified and the attacker and objectives determined, a CI occurred.[73]

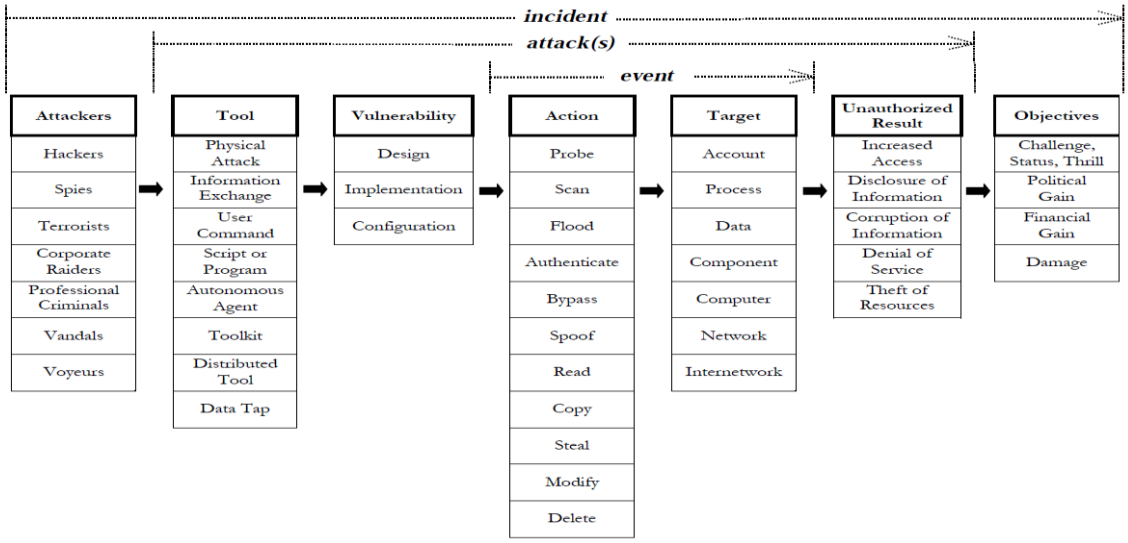
[69] Creasey & Glover, 2014, pp. 3, 11.

[70] CS event: *‘A CS change that may have an impact on organisational operations (including mission, capabilities or reputation’.* (Centre for CS Belgium, 2021, p. 6.)

[71] CS incident: ‘a single or a series of unwanted or unexpected CS events that are likely to compromise organisational operations’ (the same as the ISO 27000 on information security incident). (Centre for CS Belgium, 2021, p. 6.)

[72] Pham, 2001, pp. 1-3.

[73] Sommer, Dürrwang, & Kriesten, 2019, p. 5; Tools and vulnerabilities are first two steps used to cause an event on ICS. (Howard & Longstaff, 1998, p. 12.)



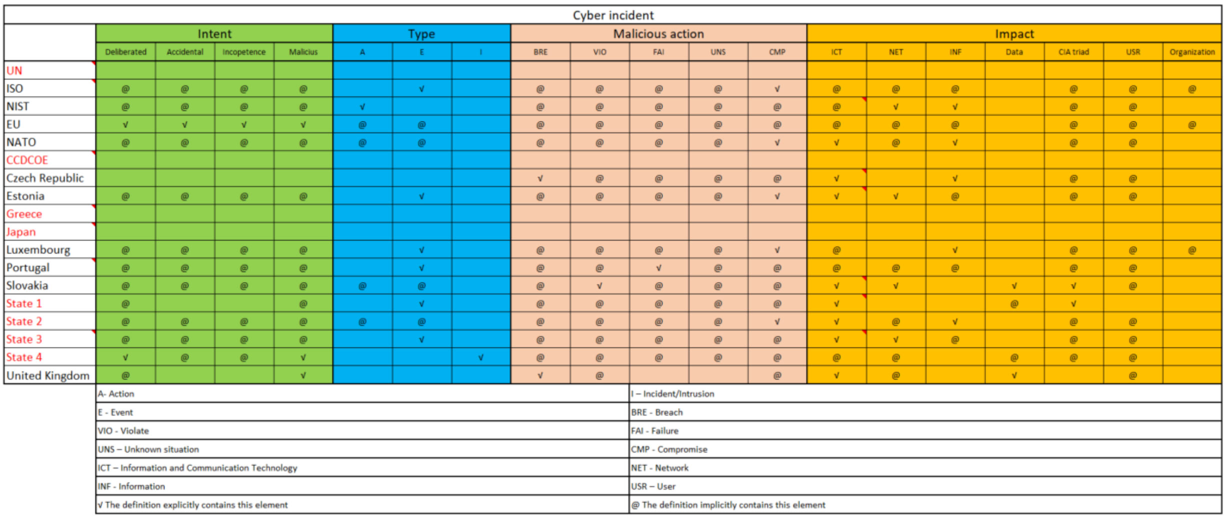
Attackers	Tool	Vulnerability	Action	Target	Unauthorized Result	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge, Status, Thrill
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomous Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

Figure 10: The Abstract CERT Taxonomy[74]

A cyber event is any identified occurrence or change in the normal behaviour of an ICS that could affect the organisation's CS policy, while a cyber attack is a precursor to a CI. A CI is declared when a cyber attack or breach actually threatens or compromises the CIA triad of an ICS and data. Therefore, an attempted cyber attack or breach per se does not constitute a CI if there is no actual impact on the CIA triad of an ICS and data. For example, an organisation that has experienced a cyber attack or attempted breach without compromising and threatening the CIA triad should not label it as a CI, but as a cyber event.

The CI concept can be compared to a cyber attack concept, hence the elements of the analysis are similar: intent, type, malicious action and impact on the subject. Table 13 shows that all entities use an agnostic approach reflecting in their very general definitions and if we ignore the explicit and implicit evaluation, then at first glance it seems that all entities have similar CI concepts, but this is not the case as they differ mainly in the labelling an incident and defining its impact on the object. The EU, NATO, Luxembourg and State 2 define CI as any occurrence[75] or an anomaly detected, which, according to the ISO and NIST, describes an event, while the Czech Republic and the UK define CI as a breach in the security of information in CIS or breach of security rules for CIS respectively. Most respondents believe that the CI is an event,[76] which is in line with expert opinion that the incident represents an escalation of the event to such an extent that the threat affects the normal functioning of the CIS and consequently the organisation. However, most respondents do not include organisation as a sub-element that can be affected by CI, which is logical, although the ISO distinguishes compromising business operations from threatening information security. Most respondents do not follow the previously explained concepts of distinguishing between information and data, nor do they follow their own concepts; for example, some of the entities in the CS concept define 'data' and in CI concepts 'information'.

[74] Howard & Longstaff, 1998, p. 16.
[75] Occurrence: the action or fact of happening or occurring (Merriam-Webster, Dictionary: occurrence, 2021, e-source).
[76] Event: something (especially something important or notable) that happens (Merriam-Webster, Dictionary: occurrence, 2021, e-source).



Cyber incident																			
	Intent				Type			Malicious action					Impact						
	Deliberated	Accidental	Incopetence	Malicius	A	E	I	BRE	VIO	FAI	UNS	CMP	ICT	NET	INF	Data	CIA triad	USR	Organization
UN																			
ISO	@	@	@	@		√		@	@	@	@	√	@	@	@		@	@	@
NIST	@	@	@	@	√			@	@	@	@	@	@	√	√		@	@	
EU	√	√	√	√	@	@		@	@	@	@	@	@	@	@		@	@	@
NATO	@	@	@	@	@	@		@	@	@	@	√	√	@	√		@	@	
CCDCOE																			
Czech Republic								√	@	@	@	@	√		√		@	@	
Estonia	@	@	@	@		√		@	@	@	@	√	√	√	@		@	@	
Greece																			
Japan																			
Luxembourg	@	@	@	@		√		@	@	@	@	√	@		√		@	@	@
Portugal	@	@	@	@		√		@	@	√	@	@	@	@	@		@	@	
Slovakia	@	@	@	@	@	@		@	√	@	@	@	√	√		√	√	@	
State 1	@			@		√		@	@	@	@	@	√			@	√		
State 2	@	@	@	@	@	@		@	@	@	@	√	√	@	√		@	@	
State 3	@	@	@	@		√		@	@	@	@	@	√	√	@		@	@	
State 4	√	@	@	√			√	@	@	@	@	@	@	@		@	@	@	
United Kingdom	@			√				√	@			@	√	@		√		@	

A- Action	I – Incident/Intrusion
E - Event	BRE - Breach
VIO - Violate	FAI - Failure
UNS – Unknown situation	CMP - Compromise
ICT – Information and Communication Technology	NET - Network
INF - Information	USR – User
√ The definition explicitly contains this element	@ The definition implicitly contains this element

Table 13: Comparative analysis definition of the Cyber Incident

A comparison of CI concepts reveals a large gap in explicitly defined sub-elements of entities (Table 13). The entities are largely unanimous only in that they define CI as an event that affects ICT and all other sub-elements are left to the reader. The EU has the most general definition, defining CI as any occurrence generated by any of cyberspace components, either natural or human-made, with malicious or non-malicious intent; deliberate, accidental or due to incompetence that affects any of the components of cyberspace or their functions. The ISO, NATO, Estonia, Luxembourg and State 2 treat CI as any detected anomaly or event that compromises ICS or business operations and threatens information security. The Czech Republic and the UK have linked CI to breaches of the CIS and CIS security rules which affect CS, respectively, while Slovakia considers CI to be a disruption of the CIS and a breach of CS security policy. Portugal has identified CI as an unauthorised or unexpected CI event where automated measures have failed but there is no severe impact on CIS.

Summarising all this, we find that the entities define CI only by one malicious act, either as a compromise, violation, failure or breach of the CIS or CS security policy. These findings are reflected in Graph 19, which shows the relationship between explicitly included and implicitly addressed sub-elements. Although the CI concept cannot explicitly include everything, it should unequivocally include all elements that compromise and threaten cyberspace, CS policy or CIA triad and the CI definition should be consistent with the CS definition. Most current CI concepts can be understood differently by the reader, which affects both the treatment and management of CI in the national and international environment.

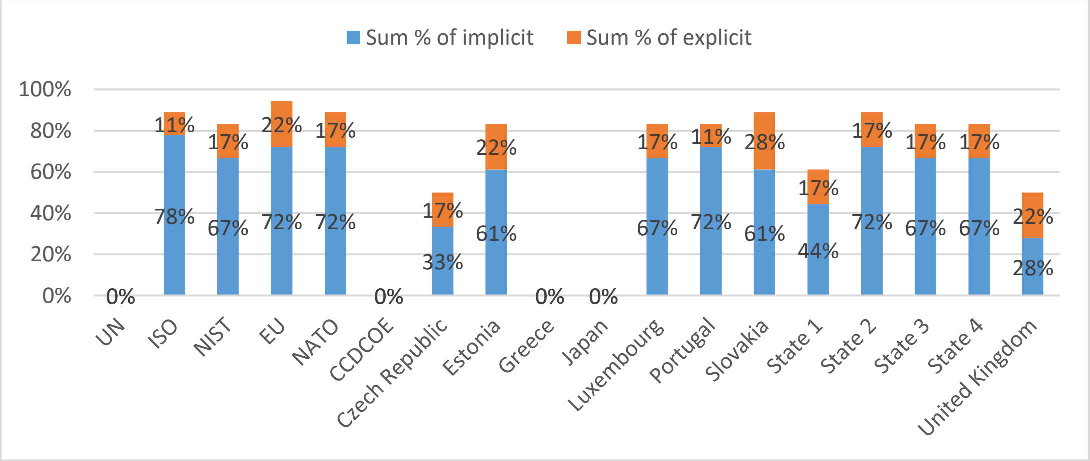
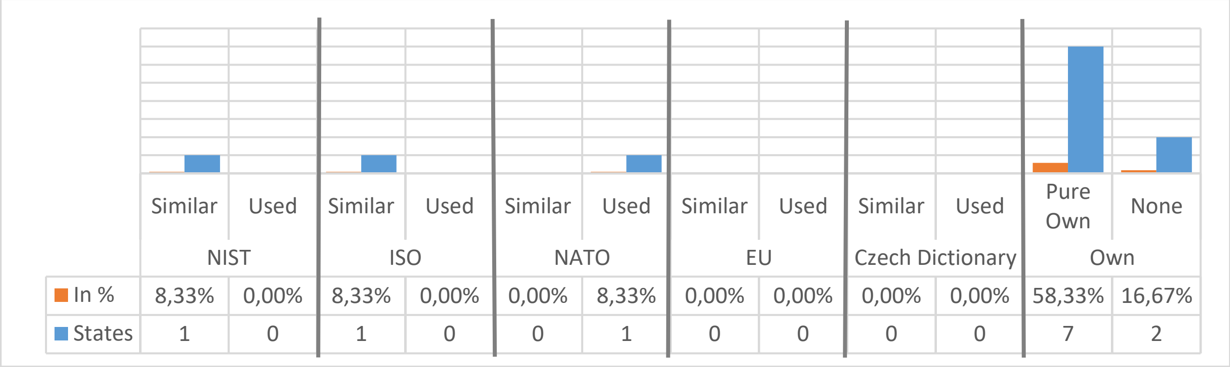


Chart 19: Explicit/ implicit included elements in the definition of Cyber Incident

The coherence of state, NATO and EU definitions of CI is reflected in Chart 20. NATO defines CI as any detected abnormality compromising or that has the potential to compromise ICS and information, and the EU defines the latter as any occurrence (including any incident generated by any of cyberspace components even if the damage, disruption or dysfunctionality is caused outside cyberspace) with any intent towards any of the components of the cyberspace or on the functioning of cyberspace. However, states use different words to define CI: either the deliberate, accidental or malicious breach, incident, information security incident, computer incident or any event, to compromise or breach either the CIA triad, INFOSEC, security rules, security of IS, communication network, information, service provision or cyberspace. Consequently, our findings show that some states do not differentiate between cyber incidents and information security incidents, which may be due to the indistinguishability between the INFOSEC concept and the CS. Therefore, based on the words used, we estimated that only State 2 uses the NATO definition verbatim and two (State 3 and Luxembourg) use a similar definition to NIST and the ISO respectively, seven have their own understanding of the CI and two do not have any definition.

Our general conclusion is that there is no common understanding of what CI is or should be and that states do not follow the concepts of organisations, which significantly affects the common international identification of violations of international law and consequently the response to CI under international law.



	NIST		ISO		NATO		EU		Czech Dictionary		Own	
	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Pure Own	None
🟧 In %	8,33%	0,00%	8,33%	0,00%	0,00%	8,33%	0,00%	0,00%	0,00%	0,00%	58,33%	16,67%
🟦 States	1	0	1	0	0	1	0	0	0	0	7	2

Chart 20: Similarity of CI definitions according to organisations' dictionaries

3.1.10 Cyber operations

According to the Merriam-Webster Dictionary, the term 'operation' is described as performing practical work or as planning and executing a military action, mission or manoeuvre.[77] Such a narrow understanding is appropriate if we consider only physical domains or a cross-domain, but we cannot agree with such a definition in the contemporary security environment. Cyberspace is primarily an environment created by civil society that states can also use as a domain of operations without the use of military units. Thus, in the broader concept of contemporary security, the concept of a cyber operation (CO) cannot be linked only to military and intelligence capabilities, but also to civilian capabilities[78] that do not necessarily belong to the Ministry of Defence or even to the nation-states. Since cyberspace has no borders, states can also execute CO through proxies or non-state actors to achieve political, social, economic or military objectives.[79] Criminal or terrorist organisations can also perform CO since they have the resources and

[77] Merriam-Webster, Dictionary: operation, 2021, e-source.

[78] The Chinese government uses both civilian hackers and military cyber units, while South Korea has a few designated governmental agency to engage to CO. (Andress & Winterfeld, 2014, p. 66, p. 93). CO is a complementary discipline to CS and it is an interdisciplinary major encompassing the entire scope of cyberspace and related technical and non-technical operations that are both (i.e., ethical, legal, human-centered, etc.). (Old Dominion University, e-source).

[79] MoD France, 2019, pp. 5-6.

organisational elements needed to perform them. In addition, significant technological advances have been made in offensive cyber capabilities as cyber operation has been shown in recent years to have a serious impact on civilian infrastructure and can cause harm to people by disrupting the provision of essential services.[80]

In armed conflict, civilian critical infrastructure (CRI) is protected by existing rules and principles of international humanitarian law (IHL), in particular the principles of distinction, proportionality and precautions in attack. However, most CO are conducted outside armed conflict to disrupt and damage civilian CRI. The International Committee of the Red Cross (ICRC) draws attention to the narrow interpretation of the term 'attack' as if the concept of attack is interpreted as referring only to operations that cause death, injury or physical damage. A cyber operation that is directed at making civilian CRI intentionally or incidentally dysfunctional thus might not be covered by IHL rules.[81] CO are politically motivated cyber attacks most commonly conducted in the form of cyber espionage, sabotage, subversion, propaganda, ransomware or cyber thefts[82] that traditionally do not violate the law of an armed conflict. The case of Estonia is clear evidence of a state-nation sponsored or undertaken cyber operation apparently funded by Russia which did not reach the level of armed conflict[83] or cause the death of people or damage to civilian infrastructure.

Harknett and Smeets distinguish CO from cyber campaigns, where CO are a series of coordinated actions directed towards a computer or network to achieve an operational objective or goals (to theft data; to cause disruption, denial, degradation, or destruction; to defend their own network), while cyber campaigns are a series of time-coordinated CO to achieve a cumulative result that leads to a strategic advantage. Therefore, CO can enable or reinforce non-CO leading to strategic outcomes and support a larger campaign to demonstrate national power.[84]

According to the Tallinn Manual and JP 3-12, CO are defined as 'the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace', while France defines a cyber operation as 'defensive or offensive cyber warfare or cyberintelligence actions'.[85] The Tallinn Manual defines a cyber attack as cyber defensive and offensive operations. JP-3-12 describes a cyberspace mission that encompasses offensive cyberspace (COO) operations, defensive cyberspace (DCO) operations and Department of Defence Information Network (DODIN) operations, and France uses terms defensive cyber warfare and offensive cyber warfare.[86] However, researchers mostly do not distinguish between offensive and defensive CO, but rather focus on the cyber operation in the general sense, which essentially means either COO or malicious cyber operation or military CO on one side and active CD on the other.[87]

Based on US Joint Publication 3-0, Dinstein and Dahl define CO as 'operations that employ capabilities aimed at achieving objectives in or through cyberspace', dividing these operations into unauthorised access to IS or networks to obtain data, but without necessarily affecting system performance (cyber

[80] Ibid, p. 208; ICRC, 2019, p. 2

[81] ICRC, 2019, pp. 2-8.

[82] Kello 2013, p. 19; Rid, 2013, p. XIV; Brantly & Smeets, 2020, p. 2, Osawa in Rõigas & Jermalavičius, 2021, pp. 2-3.

[83] Tallinn Manual 2.0 on the international law applicable to cyber operations, 2017, p. 376.

[84] Harknett & Smeets, 2020, pp. 8-9.

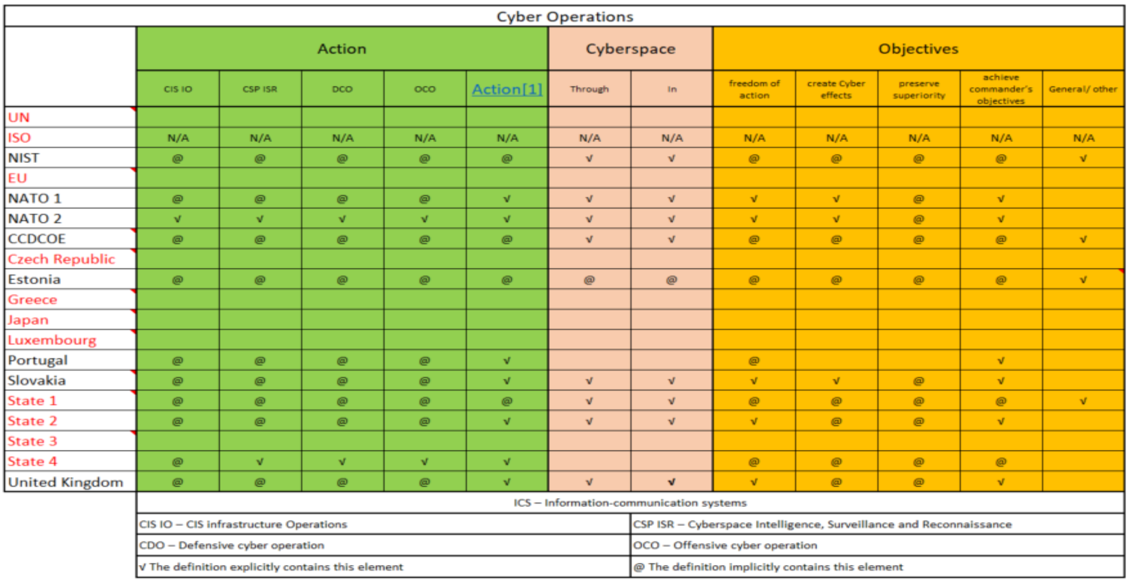
[85] Tallinn manual 2.0 on the international law applicable to cyber operations, 2017, p. 564; JP 3-12, 2018, p. VII.; MoD France, 2019, pp. 18. France: 'CO constitutes an attack if the targeted equipment or systems can no longer provide the service for which they were implemented, including temporarily or reversibly, where action by the adversary is required in order toto restore the infrastructure or the system'. 'Defensive cyber warfare: A coordinated set of actions carried out by a State which consists in detecting, analysing and preventing cyber-attacks and responding to them where appropriate.' 'Offensive cyber warfare: A set of actions carried out in cyberspace producing effects against an adversary system in order toto alter the availability or confidentiality of data'. (MoD France, 2019, p. 13, 18)

[86] Ibid.

[87] Osawa in Rõigas & Jermalavičius, 2021, p. V, 27.

espionage), and either a DCO or COO intended to compromise data or software (supporting Information operation) or to disrupt the functioning of the targeted IS or networks and related ICT-operated physical infrastructure or to produce physical damage extrinsic to the ICS.[88] Brantly and Smeets define military CO based on US Joint Publication 3-12 as an operation that nation-states' military entities plan and conduct to achieve strategic, operational and tactical advantage, divided into three categories: 1. DCO to protect, monitor, analyse, detect and respond to unauthorised activity within an IS; 2. cyber espionage operations to gather data from target or adversary IS; and 3. OCO to disrupt, deny, degrade or destroy information or the computers and networks themselves or in basic, operations designed to achieve tangible effects.[89]

These authors define CO as cyber attacks or actions and divide them according to operational objectives into DCO, OCO and cyber espionage or define them as politically motivated cyber attacks in the form of cyber espionage, sabotage, subversion, propaganda or cyber theft, including ransomware. CO also need to be understood more broadly than the military context as CO are currently being conducted in the so-called grey zone as international legal norms and rules regarding cyberspace have not yet been enacted.[90] Although recent CO are mostly politically motivated cyber attacks, the UN and the EU have not yet opted to define the concept of CO, nor have the Czech Republic, Japan, Luxembourg or State 3, while Greece[91] defines DCO and OCO. Table 14 shows that the majority of entities define cyber operation as military action, while CCDCOE, Estonia and State 1 define it in a general sense as an action or employment of cyber capabilities to achieve objectives in general. The latter approach is in line with the actual state of the contemporary security environment and has the hint of a cyber cold war as it is a tacit geopolitical and economic war using espionage, propaganda campaigns, technological competition and cyber attacks on the CRI of sovereign states without reaching the threshold of armed conflict.



Cyber Operations												
	Action					Cyberspace		Objectives				
	CIS IO	CSP ISR	DCO	OCO	Action[1]	Through	In	freedom of action	create Cyber effects	preserve superiority	achieve commander's objectives	General/ other
UN												
ISO	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
NIST	@	@	@	@	@	√	√	@	@	@	@	√
EU												
NATO 1	@	@	@	@	√	√	√	√	√	@	√	
NATO 2	√	√	√	√	√	√	√	√	√	@	√	
CCDCOE	@	@	@	@	@	√	√	@	@	@	@	√
Czech Republic												
Estonia	@	@	@	@	@	@	@	@	@	@	@	√
Greece												
Japan												
Luxembourg												
Portugal	@	@	@	@	√			@			√	
Slovakia	@	@	@	@	√	√	√	√	√	@	√	
State 1	@	@	@	@	@	√	√	@	@	@	@	√
State 2	@	@	@	@	√	√	√	√	@	@	√	
State 3												
State 4	@	√	√	√	√			@	@	@	@	
United Kingdom	@	@	@	@	√	√	√	√	@	@	√	

ICS – Information-communication systems

CIS IO – CIS infrastructure Operations | CSP ISR – Cyberspace Intelligence, Surveillance and Reconnaissance

CDO – Defensive cyber operation | OCO – Offensive cyber operation

√ The definition explicitly contains this element | @ The definition implicitly contains this element

Table 14: Comparative analysis definition of the Cyber Operations

Table 14 shows that only NATO and State 4 explicitly define cyber operation actions such as CDO, OCO, cyber intelligence, surveillance and reconnaissance, and NATO also defines CIS infrastructure operations. The essential difference between the definition of NATO and State 4 is the cyber operation objectives as State 4's objective is to gain a tactical advantage in cyberspace, while NATO aims to create

[88] Dinstein & Dahl, 2020, p. 19.

[89] Brantly & Smeets, 2020, pp. 3-4.

[90] Rice, Butts, Shenoi, 2011, p. 58.

[91] DCO: 'is the sum of safeguards, procedures and actions that are applied for the protection of the National Cyberspace.' OCO: 'are the actions-activities that are conducted with intent to dominate over the opponent's cyberspace.' (Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021).

cyber effects to achieve the Commander's objectives and preserve freedom of action in cyberspace, however, there is no explanation what cyber effects are or which cyber capabilities are considered, only military or military and civilian. Therefore, we used a taxonomy of cyber effects and put them into physical, digital, economic, psychological, political, reputational, social and societal categories that can be achieved through actions such as deny, degrade, disrupt, destroy, manipulate and espionage.[92] We have used Couretas's description of cyber effects and military activities in connection with the CIA+ triad: interruption (availability), modification (integrity and authenticity), degradation (availability), fabrication (integrity and nonrepudiation), interception (confidentiality) and unauthorised use (not considered) that can be achieved via military activities as deny, degrade, disrupt, destroy, espionage, DCOand OCO (cyber attack: deny, degrade, disrupt, destroy, espionage).[93] We evaluated how the entities implicitly conduct all activities to achieve military objectives; however, we did not include general objectives (the broader context of CO and politically motivated cyber attack), unless the latter was explicitly included in this definition. The analysis of CO concepts also shows that entities carry out actions or activities and use cyber capabilities to achieve a goal, leaving it up to the reader to define the types of activities and other goals. Therefore, our estimate does not necessarily match the estimation of the author of the cyber operation definition or another reader.

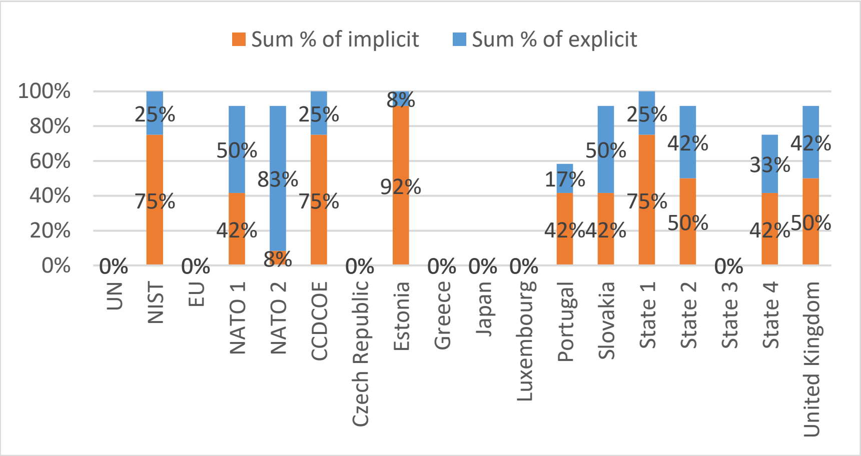
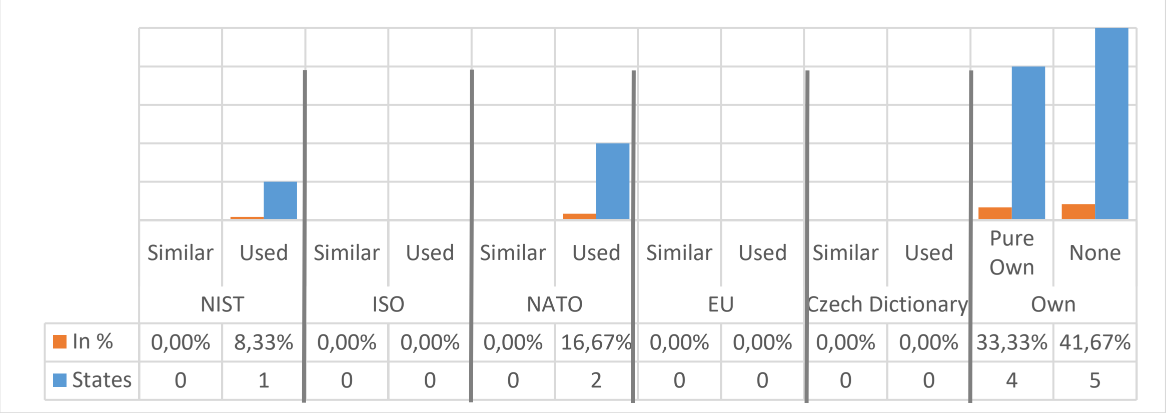


Chart 21: Explicit/ implicit included elements in the definition of CO

Although at first glance it appears that the CO concepts of the actors are similar, the analysis shows otherwise. The NATO concept explicitly defines four areas of CO, focusing on preserving own and friendly freedom of action and achieving the Commander's objectives. The NATO concept is followed verbatim by State 2 and Slovakia, but Slovakia does not clarify which NATO definition is used as NATO has two. The UN and EU do not have a cyber operation concept, four entities do not have a cyber operation concept, while the Czech Republic withheld this information. NIST defines cyber operation in a general sense and does not focus on military objectives and this concept is followed by State 1, while Estonia, Portugal, State 4 and the UK use their own definitions. Estonia focuses on activities in the networks and IS environment, Portugal on achieving military goals using cyber capabilities, State 4 on gaining tactical advantage in cyberspace and the UK on planning and synchronisation of activities in or via cyberspace to enable freedom of manoeuvre and to achieve military objectives. Thus, entities have different cyber operational concepts that are not in line with the NATO concept itself and also not between entities, which makes it difficult for common planning and conduct of NATO CO, especially those which do not reach the threshold of armed conflict (cause injury or death to persons or damage or destruction to objects).

[92] Orye & Maennel, 2019, p. 13. Cyber effects on the cyber adversary: redirect (deter, deceive, divert), obviate (prevent, pre-empt), impede (degrade, delay), detect, limit (contain, recover, curtail, expunge), and expose (analyse, publicise). (Bodeau & Graubart, 2013, p. 8).

[93] Couretas, 2018, p. 37.



	NIST		ISO		NATO		EU		Czech Dictionary		Own	
	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Similar	Used	Pure Own	None
🟧 In %	0,00%	8,33%	0,00%	0,00%	0,00%	16,67%	0,00%	0,00%	0,00%	0,00%	33,33%	41,67%
🟦 States	0	1	0	0	0	2	0	0	0	0	4	5

Chart 22: Similarity of 'cyber operation' definitions according to organisations' dictionaries

3.1.11 Aggression

ICT, cyberspace, IE, cyber threats and hybrid threats are some of the contemporary sources of threats, mostly in the form of non-military threats and the perpetrator is difficult to attribute. The common denominator is a cyber attack in the form of cybercrime, cyber terrorism or a cyber operation that can reach a level of aggression and consequent armed conflict. However, the contemporary security environment no longer consists only of the physical dimensions of space, but also of man-made artificial space. Considering rationalist and constructivist theory,[94] these threats were detected or securitised so we are interested in whether the entities have taken this into account in national documents and redefined the concept of aggression.

While the qualification of cyber attack under international criminal law has not yet been determined, it is consensual that international law in the context of jus ad bellum and jus in bello also applies to cyberspace.[95] Such a position is taken by the International group expert, which also believes that the UN Security Council could decide that certain types of cyber operations violate the UN Charter 'in abstract', which it has not done so far.[96] In addition, they concluded, that a cyber attack or cyber operation conducted by individuals or non-state actors, civilian or military, can be qualified as a war crime if they meet the objective (criminal act – actus reus) and subjective (criminal intent – mens rea) criteria.[97]

The Merriam-Webster Dictionary defines aggression as a forceful action or a procedure aimed at domination and master; or the practice of attacks or encroachments in the form of unprovoked violations of territorial integrity; or a hostile, injurious or destructive behaviour or outlook.[98] The concept of aggression is also defined in Article 1 of the UN Charter and in more detail in Resolution 3314 as acts against peace committed by the armed forces to violate the sovereignty, territorial integrity or political independence of another country.[99] Mendoza states that cyber attacks are acts of aggression if they are conducted by cyber units of another country, while Ophardt, Morris and others point out the need to revise international law and include a non-military threat component and to incriminate all crimes in or through cyberspace to recognise the importance of below the threshold aggression, especially in the grey zone.[100] However, current state practice is to conduct cyber attacks or cyber operations in the grey zone to which

[94] Realistic theory addresses the perception of state actors leading to the securitization of the security issue, while constructivist theory analyses the process of potential threat to the general public. (Scheerder, 2012, p. 82).

[95] Greco, 2020, p. 40.

[96] Tallinn manual 2.0 on the international law applicable to cyber operations, 2017, p. 357.

[97] Ibid, p. 176, pp. 392-393).

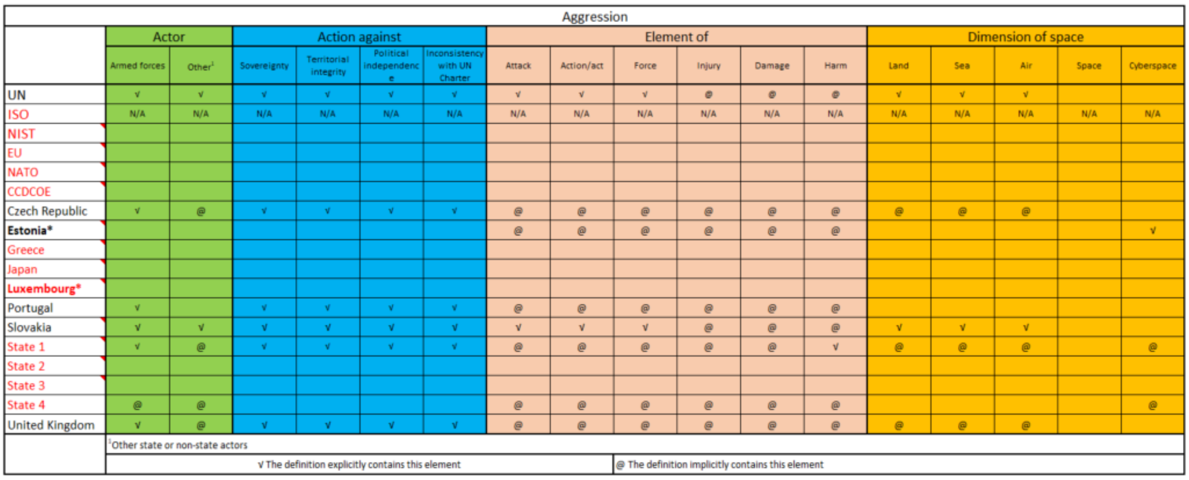
[98] Merriam-Webster, Dictionary: aggression, 2021, e-source.

[99] United Nations General Assembly Resolution 3314 (XXIX), April 1974.

[100] Ophardt, 2010, pp. 9 -12; Mendoza, 2017, pp. 17-19; Morris et al., 2019, pp. 2-5. Morris et al stress that allies must decide what actions in the grey zone environment they will not resolutely tolerate. (Morris et al, 2019, p. XVII)

the law as it exists does not apply as a cyber attack is not yet internationally legally defined and the narrow understanding of cyber attacks is not in conformity with the principles of international law that protect civilians from direct attacks.

Table 15 is divided into four main and 17 sub-elements. The purpose of this analysis is to determine whether states have altered their own definitions of aggression due to a complex security environment or how they perceive aggression in a changed security environment. It shows that nine of the 17 entities have not defined the term aggression, while the Czech Republic, State 1 and the UK refer to Article 1 of the United Nations General Assembly Resolution 3314, therefore other sub-elements are also implicitly included. In addition, State 1 separately defined cyber aggression as intentional harm via electronic means to people without including other elements of cyberspace, while Slovakia has a generally accepted understanding, without justifying it. Japan replied that the term ‘aggression’ is not universally accepted and Luxembourg replied that it preferred to use the definition of the EU and NATO, which they have not yet defined. Estonia and State 4 associated the concept of aggression with cyber operations or actions in or through cyberspace. Estonia defined aggression as action in or via cyberspace that projects power to create effects to achieve military objectives, while State 4 took a wider approach and defined aggression as any offensive operation targeting their network.



	Aggression																
	Actor		Action against				Element of						Dimension of space				
	Armed forces	Other[1]	Sovereignty	Territorial integrity	Political independence	Inconsistency with UN Charter	Attack	Action/act	Force	Injury	Damage	Harm	Land	Sea	Air	Space	Cyberspace
UN	√	√	√	√	√	√	√	√	√	@	@	@	√	√	√		
ISO	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
NIST																	
EU																	
NATO																	
CCDCOE																	
Czech Republic	√	@	√	√	√	√	@	@	@	@	@	@	@	@	@		
Estonia*							@	@	@	@	@	@					√
Greece																	
Japan																	
Luxembourg*																	
Portugal	√		√	√	√	√	@	@	@	@	@	@					
Slovakia	√	√	√	√	√	√	√	√	√	@	@	@	√	√	√		
State 1	√	@	√	√	√	√	@	@	@	@	@	√	@	@	@		@
State 2																	
State 3																	
State 4	@	@					@	@	@	@	@	@					@
United Kingdom	√	@	√	√	√	√	@	@	@	@	@	@	@	@	@		

[1]Other state or non-state actors

√ The definition explicitly contains this element

@ The definition implicitly contains this element

Table 15: Comparative analysis definition of the Aggression

Thus, we can conclude that there are states that follow existing law and others that have specifically defined aggression in action in or via cyberspace. Notwithstanding the above, the so-called grey zone is the reflection of an opinion of law (opinio juris) and states practice in perceived violations of compelling law (jus cogens) and crimes under international law, therefore states need to define cyber aggression in national legislation as in this way they formulate and establish international law through their own practice.

3.2 Legal and institutional framework

Security is a fundamental element of any democratic society, but must be based on legal principles and norms that are acceptable to the wider international community. This is especially important in today's security environment, which is complex and has changed significantly. In addition to the physical dimensions of space, there is also an artificially created dimension called cyberspace. If we want to establish an appropriate legal and institutional organisational framework (security architecture) for CS and defence, then a comprehensive approach is needed as shown in Figure 1. This comparative analysis addresses all levels of security architecture in twelve states, from top-down or from information assurance towards protection CRI respectively.

The legal framework includes rules, rights and obligations of nations' entities set out in constitutions, legalisation, policy, regulations and contracts,[101] while the institutional framework refers to formal law or other provisions that shape the activity and behaviour of entities.[102] States were asked to provide data on cyber-related concepts: IA, INFOSEC, CS, CD, hybrid threats and protection of CRI. Chart 23 visualises the legal framework of states regarding the provision of security and defence of all five spatial dimensions. According to the collected data, only one state out of 12 has all legally regulated and directly related areas to cyberspace (but if we ignore hybrid threats (HTs), there are five states). The least regulated areas of most states are HT, IA and IS. This is likely a reflection of different perceptions of cyber-related concepts or due to the rapid changes in the security environment that these states have yet to address. However, from the responses received, it could be that states generally implement security measures in different cyber-related concepts. However, some states believe that there is no difference between IA and INFOSEC or that IA deals with the protection of classified information and systems. These states that do not have a specially adopted legal framework in the field of IA regulate this field with legislation within the framework of INFOSEC and a similar analogy can also be observed in the relationship between IS and CS.

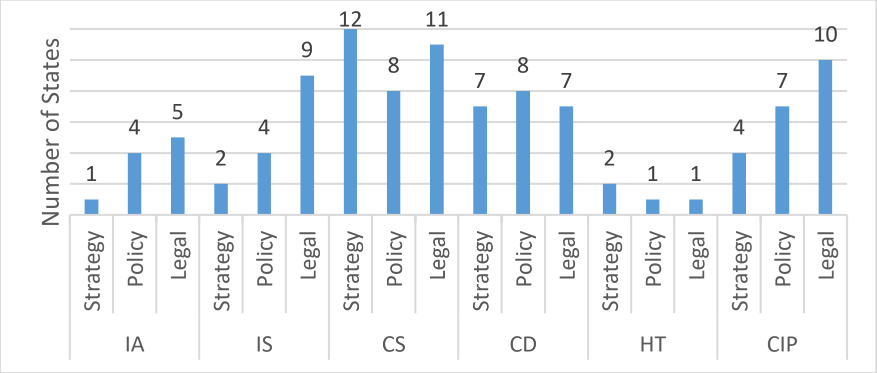


Chart 23: Overview of the Legal framework by Cyber-related concepts of states

The most formally regulated areas are CS, CD and critical infrastructure protection (CIP), and all states have adopted a CS strategy. Seven have a CD strategy and four have a CIP strategy. Some also use their CS and CD strategy as a policy document, while three have also adopted an action plan for the implementation of these strategies or special regulations and programmes for CS and CD. Most use the same legal framework for IS and CS or an IA framework despite recognising IA, IS and CS as separate concepts. In the field of IS, personal data protection and CIP, EU Member States follow EU regulation by implementing or transposing EU regulations (General Data Protection Regulation-GDPR and EU Network and Information Security (NIS) directive) in their national legislation.

While legal and institutional frameworks seek to shape activities and behaviours of entities under national and international law, some standards establish structures of uniform sets of rules for the measurement of quantity, weight, extent, value or quality.[103] These standards can be national (e.g. NIST, IT-Grundschutz, ISKE) or international/multinational (e.g. ISO, EU, NATO). However, a state is not obliged under international law to apply any standard in a unified approach to CS and defence. As shown in Chart 24, the most used standards are national standards (purely national and derived from national legislation, i.e. NIST, ISKE, ITIL) followed by the ISO27XXX series, the ISO 27001 and other international/multinational standards such as IASPs (International Association of Science Parks and Areas of Innovation), EU IASGs (Impact Assessment Steering Groups), eIDAS (electronic IDentification, Authentication and trust Services), NATO Vulnerability Assessments and Penetration tests. These states

[101] NRGI, 2015, p. 1.

[102] OECD, 2021, e-source.

[103] Merriam-Webster, Dictionary: standard, 2021, e-source.

use the same set of standards across IA, IS and CS, while within the area of CD they mainly use NATO policies and standards.

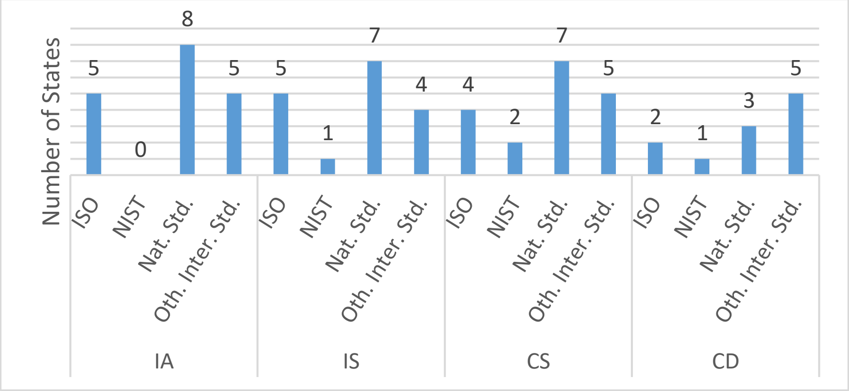


Chart 24: Standards use by states

Within the realm of legal and institutional cyber frameworks and standards, security audits also need to be defined. According to NIST, a security audit is an 'independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services and recommend any changes that are indicated for countermeasures'.[104] Security audits should be performed periodically or continuously by internal (a department within a larger organization) and/or external entities (auditing firms or regulatory agencies) to show the efficiency of the organisation's implemented security policies and to reveal possible gaps and vulnerabilities in their current systems and procedures, thus ensuring and maintaining integrity and quality of systems and data/information.[105] As Graph 25 shows, the majority of respondents conduct annual audits of all cyber-related concepts. In the areas of IA and IS, four states do not perform any audits, three perform both internal and external, and five either conduct only internal or external audits. Almost the same picture can be seen in CS, where three states perform both internal and external audits, three do not perform any audits and six only conduct either internal or external audits. CD, however, is a completely different situation: six states do not plan any audits, two plan both external and internal and finally only four either plan internal or external.

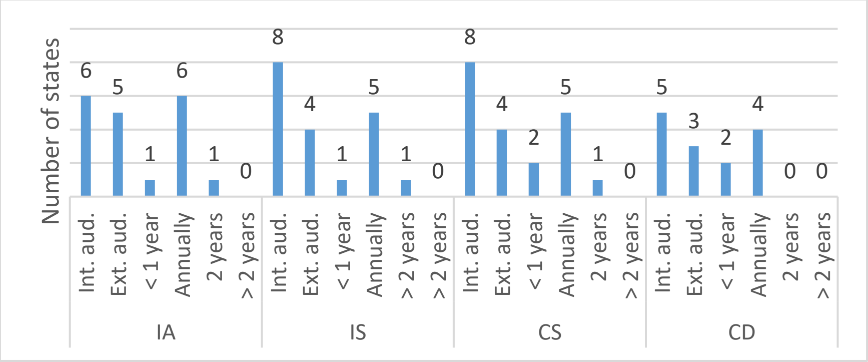


Chart 25: Overview of the Planned Audits

3.3 Organisational framework

The security of a state depends on several different stakeholders and their roles, which are set out in their legal and institutional frameworks. As a result, states have developed different organisational frameworks

[104] NIST, Glossary: Security Audit, 2021, e-source.
[105] Goel, Pon & Menzies, 2006, p. 26.

that consist of an organisation's structural components and their internal and external interactions. States' frameworks are either centralised or decentralised organizational structures that consist of activities directed towards the achievements of that organisation's aims.[106] These activities can be rules, tasks, roles and responsibilities to execute, integrate, coordinate and supervise the efforts of all stakeholders at all levels.[107] The organisational framework should also include a four-level model of security governance, from the policy level down to the tactical (technical) level (Figure 11).[108] This four-level model was used by Klimburg to delineate the organisational functions, capabilities and responsibilities of a national CS framework in five basic mandates: '(1) Internet Governance and Cyber Diplomacy, (2) Cyber Crisis Management and CIP, (3) Military CO, (4) Intelligence/Counter-Intelligence and (5) Counter Cyber Crime'.[109]

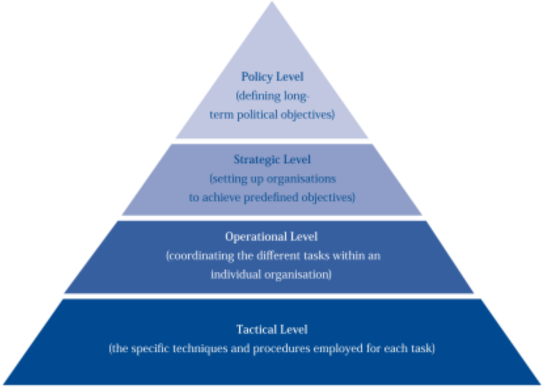

Policy Level
(defining long-
term political objectives)
Strategic Level
(setting up organisations
to achieve predefined objectives)
Operational Level
(coordinating the different tasks within an
individual organisation)
Tactical Level
(the specific techniques and procedures employed for each task)

Figure 11: The four levels of security governance[110]

Chart 28 shows the states' governance of their IE or their organisational structure of the IE, including the areas of IA, IS, CS, CD and HTs. The role of IA governance in seven states is allocated to a governmental body such as national security authority (NSA), classified data protection authority, national cyber and information security entity (NCIE[111] or national or military intelligence service. In addition, individual states have IA governance distributed between the NSA and the NCIE/security and intelligence services or even between several different government bodies. Despite there being different organisational structures among various states, their common role is to issue security clearances and protect classified information and CIS. This is accomplished by formulating IA policy and implementing physical, personnel, administrative, industrial, CIS and crypto security.

[106] Elsaid, Oksaha, & Abdelghaly, 2013, p. 1.

[107] Maheshwari & Agrawal, 2020, p. 196; Elsaid, Oksaha, & Abdelghaly, 2013, p. 1.

[108] Klimburg, 2012, p. 111.

[109] Ibid, p. 110.

[110] Ibid, p. 111.

[111] E.g. National Cybersecurity Centre, National Informational Security Centre.

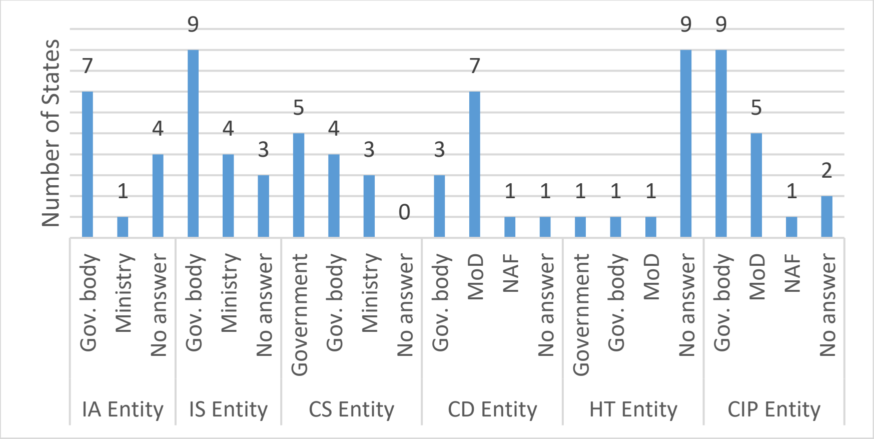


Chart 26: Governance of Information environment

The IS field has a similar organisational structure as IA, however four of the twelve states have distributed roles between governmental bodies and ministries and five have IS governance solely at the level of governmental bodies (Chart 28). Some states have the same entities for IA and IS (such as the NSA and NCIE), while others have established special entities in the form of an IS or IT directorate, administration or office. Two have distributed IS governance across various ministries responsible for CIS, e-services, security and education, while three did not provide any answers. Unlike IA governance, due to different IS organisational structures and lack of information received, it is impossible to identify common tasks, especially since some states have the same entities in both fields and therefore the roles are the same. Those states that responded mainly gave generic answers regarding the roles of individual ministries or government bodies related to their tasks such as IS/national ICT governance, creation of information security standards and policies, digital transformation, education, security and IS coordination.

The governance of CS is divided between the government, various governmental bodies and ministries. In five of the 12 states, the government is responsible for CS, for four states the governmental body (National Cyber Security Centre (NCSC), NSA, agency, Security Council) is responsible in three states the Ministry is designated, while three states did not provide an answer (Chart 28). However, all states have a multi-level approach from the political-strategic level down to the technical level. Five states have an intelligence service in their national IS system and some states have included national security committees and set up special CS committees or councils. In addition, most have a Ministry of the Interior and Ministry of the Foreign Affairs, a Ministry of Defence (MoD) and a Ministry responsible for the ICT involved in the national IS system. The roles and responsibilities of each entity are in accordance with their basic tasks or responsibilities.[112]. The political-strategic level is responsible for analysing the national security situation and developing a national CS and CD framework. The operational level is responsible for the implementation of CS and CD policies and the effective execution of CS and CD measures at the technical or tactical level.

CD is another field that shows diversity in organisational structures of the observed states. Three of the twelve states have assigned CD governance to governmental bodies (Security Council/Committee/Agency), seven to the MoD/Intelligence Service, one to the National Armed Forces (NAF) and one state has decided not to answer (Chart 28). In this regard, the roles and responsibilities of the entities differ as the CD organisational structure of states is differs across multiple levels. Nevertheless, they all have in common that the MoD and NAF are responsible for conducting national defence and CO (while other roles and responsibilities could not be analysed due to a lack of input data from the participating states).

[112] E.g. Ministry of Interior for cyber safety and fight against cybercrime, Ministry for Foreign Affairs for Cyber diplomacy, ect.

Four have established a NCSC and seven a National Cyber Forces (NCF) or Cyber Force Command (CFC) or Cyber Defence Centre (CDC) as is shown in Chart 27. The location of the NCSC differs between states, with two forming an independent government body and one having it with the national intelligence service. Additional to the NCSC, three have established NCF within the NAF, one has the National Cyber Operations Centre within the military intelligence service, two have the Cyber Defence Centre within the NAF or military intelligence service and one has a Cyber Defence Unit in the National Guard.

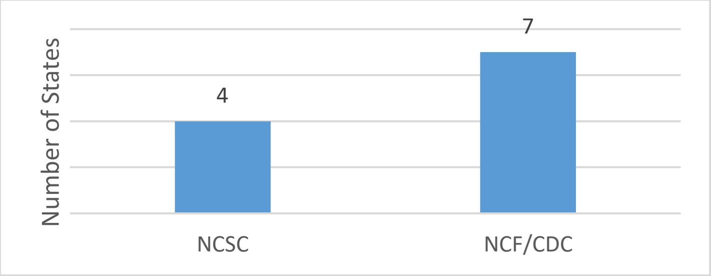


Chart 27: Overview of States´s CD capabilities

Little data were obtained in the field of HT. Of the 12 states, nine did not provide any response regarding organisational structure (Chart 28). The other three states designated HT governance either to the government or government bodies or the MoD. All three included either the national Security Council or intelligence service as an advisory body, while one had established a centre against terrorism and HT under the Ministry of Interior. One state included the Ministry for Foreign Affairs to cover political aspects of HT and two included the MoD as an operational body to counter HT.

At first glance, CIP entities do not differ significantly between states (Chart 26). Most states have defined government entities that are tackling the issues with CIP, but these entities differ (NCIE, national CERT, public and private CERTs, government secret service or representatives of sectoral ministries). By contrast, some government entities just have a role to coordinate between other entities whereas some also have responsibilities in performing CIP in response to a cyber incident. Finally, some states also include the MoD (particularly the associated intelligence service) with the responsibility to counter or mitigate cyber attacks.

3.3.1 Nation's or organisation's role in cyber defence

To define the role of the state or organisation in CD, it is necessary to establish an operational framework that describes how the state or organisation will manage it. Due to the lack of data from the surveyed states, we could only make an overview of inter-ministerial roles at the working level in which entities are defined as dedicated, centralised and coordinated bodies for a nation’s CD.

At the operational inter-ministerial level, seven states have councils, ad hoc groups or special entities. In two, the government or the MoD is designated at the operational inter-ministerial level and in one case it is the Ministry responsible for ICT (Chart 28). In addition, one state follows a principle of decentralisation as each entity provides its own CD, however, the coordination body is NCIE.

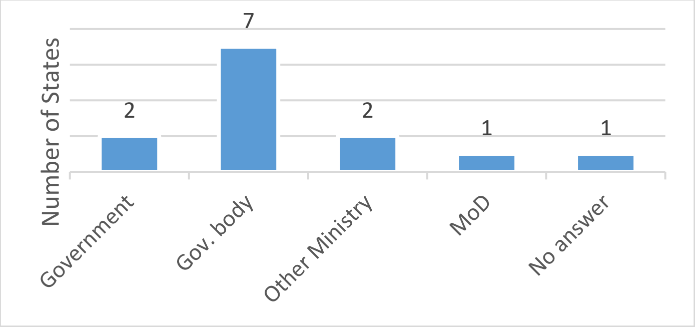


Chart 28: Distribution of CD competencies at the operational inter-ministerial level between various government entities

Regarding national CD at the working level, nine of the twelve states have included their MoD and NAF and seven states have other ministries such as a Ministry of Foreign Affairs, Ministry of the Interior or the Ministry responsible for ICT, other governmental bodies such as national cyber or information security centres or various agencies and ad hoc groups. Four included intelligence services at the working level, either national or military, and six also national or other CERTs.

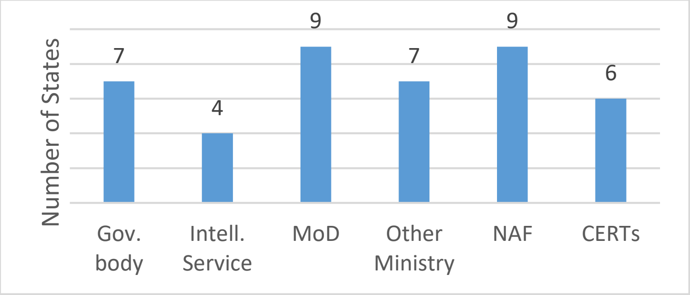


Chart 29: Distribution of CD competencies at the working level between various government entities

As shown in Chart 30, most states have both dedicated and centralised bodies for CS and CD, while one state did not provide an answer. Most did not say whether they have dedicated or centralised bodies for CS and CD, but listed all entities involved in the national CI response system: the MoD, CERTs, the ministry responsible for ICT, the Ministry for Foreign Affairs, the police and other relevant government bodies including intelligence services. Therefore, based on the responses of the states, we assessed for ourselves whether it is a dedicated or centralised body. We found that nine countries have dedicated bodies for CS in the form of NCSCs, agencies, their nation's relevant Ministry of ICT and CERTs; two states do not have a centralised body; and one state did not respond. Most have the same entities for designated and centralised CS bodies, with two stating that it is a semi-centralised and shared responsibility of the MoD and the Ministry responsible for ICT. One stated CS was a joint effort across all relevant entities, while two states do not have centralised bodies.

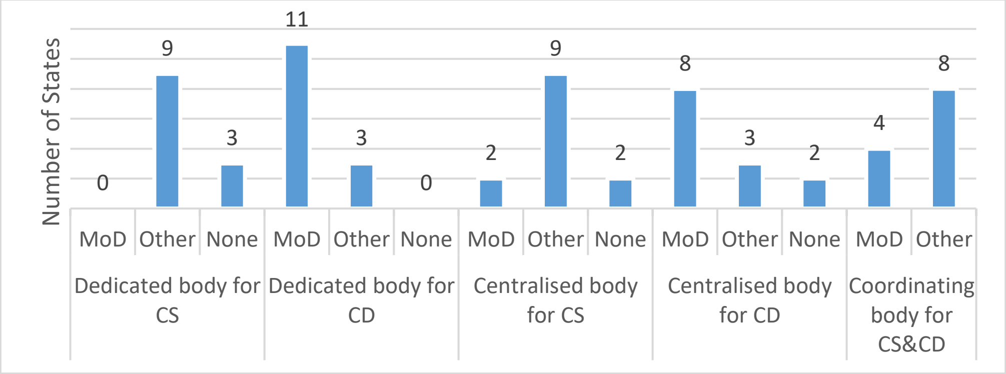


Chart 30: An overview of nations' government bodies on CS & CD

In most states, the governance and implementation of the national CD are left to the MoD and its subordinate organisations including the NAF and military intelligence, within which states have formed dedicated and centralised bodies such as the Directorate of CS, MoD Strategic Command, the National CS Centre or cyber units for CD. Three states stated that national CD is a shared responsibility of MoD and the Ministry responsible for ICT, two states see national CD as a joint effort across relevant government entities, while two states do not have a centralised body for CD. One state responded that each government organisation is responsible for its CD but coordination was conducted by NCIE.

Coordination for CS and CD varies greatly between states (Chart 30). Two defined different coordination bodies at the political (cabinet of ministries), strategic (MoD or its subordinate bodies) and operational (NAF or NCSC) levels. Other states have a CS and CD coordination function divided between their MoD and the Ministry responsible for ICT with political oversight by the Council, NCIE, IS authority, inter-ministerial coordination committee and ad hoc groups (police, intelligence service, NCSC and CDC). This shows that in two cases the MoD is an independent coordinating body and in two others it is solely at the strategic level. In all other cases, different government entities are designated for the coordination of other intra-governmental bodies.

For crisis response management at the national level (including HT), all states include the MoD and CERT, while eight also include other government bodies such as the NCSCs, relevant agencies and crisis units, national or military intelligence services (Chart 31). Three said that the government (prime minister or cabinet of ministers) and NAF should be involved in crisis response, while two also included other ministries (Ministry of Interior, the Ministry responsible for ICT and CIP). According to the responses, the main role of government was making decisions, while other government bodies have a role in either coordinating activities or serving as a single point of contact.

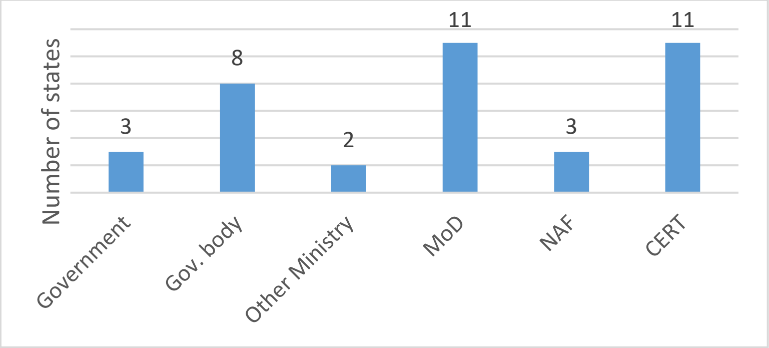


Chart 31: Cyber defence at the national level (including HT)

3.4 Capabilities

Capability is ‘the quality or state of being capable’[113] or ‘the ability to do something’.[114] Concerning cyber capabilities, NIST takes into account only the technical aspect of cyberspace as only the CIS, which is designed to generate cyber effects in/through cyberspace, is considered as cyber capabilities.[115] However, cyber capabilities are not only the technical level of cyberspace (cyber weapon) but also resources and assets that can be used to resist or exert influence in cyberspace by using ICT.[116] A similar understanding was taken by the Australian Strategic Policy Institute, which identified capabilities in the context of cyber operation: ‘having a capability means possessing the resources, skills, knowledge, operational concepts and procedures to be able to have an effect in cyberspace’.[117]

Notwithstanding the above, the analysis conducted only observed the elements of resources and knowledge, focusing on shared CS, pure CD and future CD capabilities. The analysis of CS capabilities shows that five states (42 %) have shared CS capabilities at their Ministry responsible for ICT and ten states (83 %) at government bodies such as national CERT and NCIE, with no data from one state. Two included their Ministry for CIP and four included their MoD (33 %). However, a detailed analysis in Chart 32 shows that three states (25%) dispersed their shared CS capabilities between different entities, namely: the CS capabilities of the Ministry responsible for ICT (17%), government bodies (58%) and MoD (33%), with the latter is responsible for responding to CIs on defence networks. An analysis of their mission has not been conducted due to the lack of information from participating states. Nevertheless, five responded that the ministries responsible for ICT and CIP coordinate CS incident responses (33%), while the government body’s role is to respond to cyber incidents for the civilian networks (67 %).

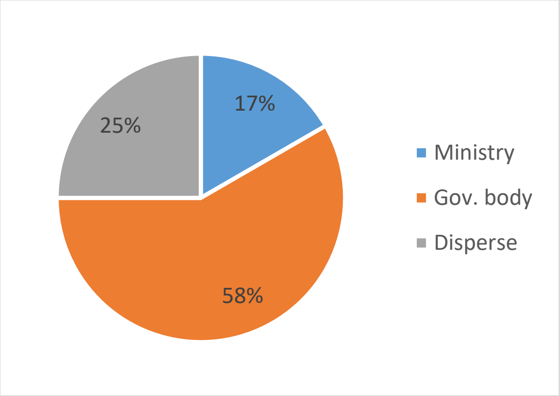


Chart 32: Shared CS capabilities

Most states allocated pure cyber capabilities (including decision-making) to different entities: their Ministry responsible for ICT or government bodies such as the national CERT, intelligence service, NCSC or a directorate/department of the MoD or NAF (Table 16).

Entity	Role
1. MoD 2. Other bodies under MoD	1. National CD against severe cyber attacks, military cyber operation and response to cyber attacks, defensive cyber operation; 2. Coordinates CS/CD issues, sets policies, standards, procedures etc.

[113] Merriam-Webster, Dictionary: capability, 2022, e-source.
[114] Cambridge Dictionary, Dictionary: capability, 2022, e-source.
[115] NIST, Glossary: cyberspace capability, 2022, e-source.
[116] Craig, 2020, p. 58.
[117] Australian Strategic Policy Institute, 2022, e-source.

NAF: 1. NCOC, CDC 2. MilCERT 3. Cyber Command 4. Cyber Unit	1. Executing national CD; response to serious cyber incidents (including CIP); 2. Cyber incident response on military networks; 3. Military CO, protects cyberspace and response to cyber attacks; 4. CD of NAF, protects cyberspace and responds to cyber attacks.
Intelligence service	1. Executing national CD; 2. National CD authority.
Other government bodies (National CERT, NSCS)	1. Crisis response on civilian networks (including CIP); 2. CD on the civilian networks; 3. CS and CD coordination body.
Ministry responsible for ICT	1. CD on the civilian networks.

Table 16: Roles of Pure CD entities

Seven (58%) states out of twelve answered that national CD is a shared responsibility, while just three (25 %) is imposed it on their MoD, NAF or military intelligence service (Chart 33). However, none of the surveyed state responded to the role of the MoD/NAF in peacetime, but as is shown in Table 16, most states answered in a general sense. In this regard, all states are in favour of the MoD/NAF being generally responsible for CD on MoD/NAF networks and conducting CO, while civilian entities are responsible for civilian networks. In addition, two states advocate national CD as a joint effort across relevant government entities, while three follow the Klimburg model by subordinating the national CD body to their intelligence service (two states to military intelligence and one to national intelligence). Five states have formed offensive cyber capabilities, five have not and three refrained from responding (Chart 34).

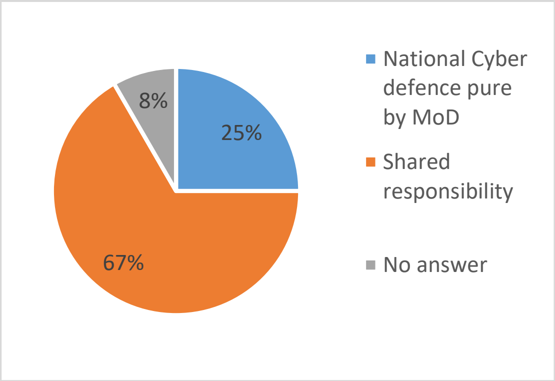


Chart 33: National Cyber Defence

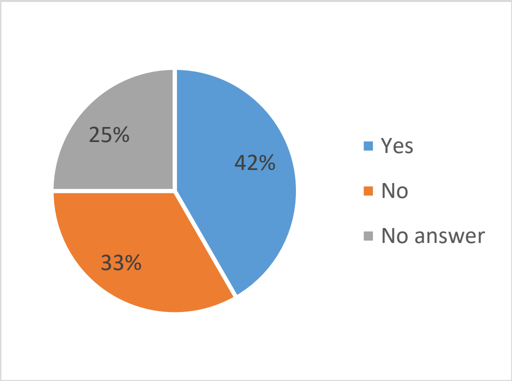


Chart 34: Current Offensive cyber capabilities

With regard to interoperability[118] (Chart 35), three states did not provide any answers and six linked interoperability with the implementation of EU and NATO policies and standards and participation within various projects at the policy and capacity levels. One follows interoperability by following systems requirements defined by NATO, one uses NATO AJP 3.20 and one sets policy to be interoperable with other international entities.

[118] In this study interoperability means that States following EU/NATO documents, policy and guidelines.

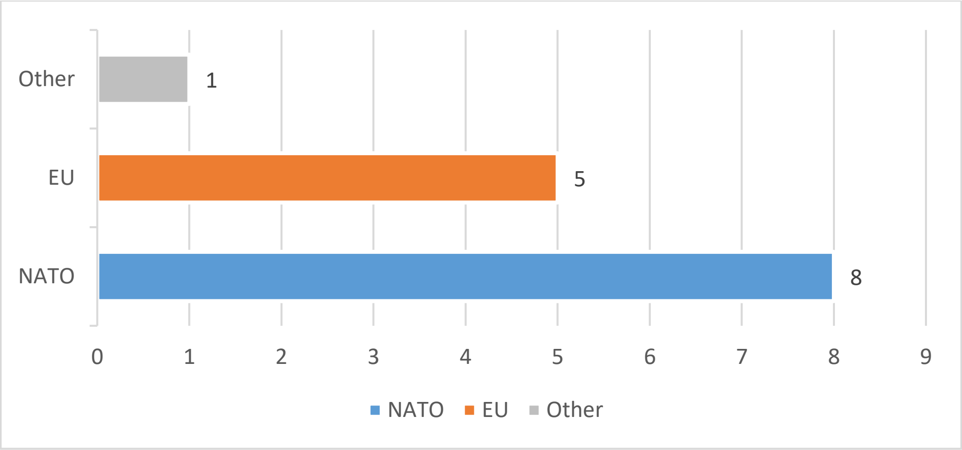
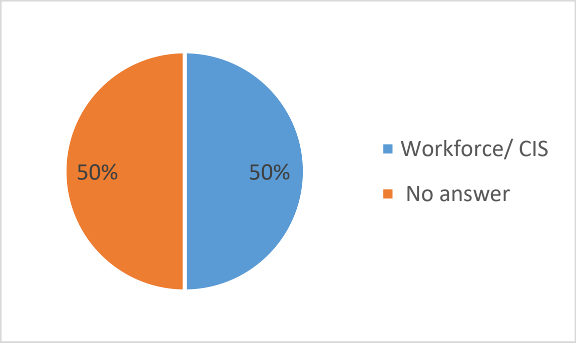


Chart 35: Interoperability

Six states said they would build future cyber capabilities within the defence sector, while six states did not answer (Chart 36). These capabilities will focus on CR, active CD (including artificial intelligence), full-spectrum operations (including a Cyber Operational Picture), educational capabilities and cyber effects capabilities. Three will also build offensive cyber capabilities, while nine have refrained from answering this question.



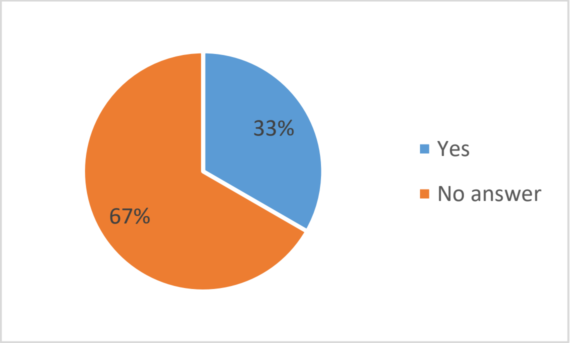


Chart 36: Future cyber capabilities

Chart 37: Future Offensive cyber capabilities

3.4.1 Human resource management

Ensuring the security of the IE and cyberspace is not only a technical challenge in building cyber capabilities, but also in human resource management (HRM). The essence of HRM is a strategic approach to the effective and efficient management of people in the organisation, to gain a competitive advantage and increase employee performance.[119] Organisations need to define an HRM strategy that encompasses benefits, recruitment, training and development, performance appraisal and reward management.[120] Nowadays, many states and private companies are facing attraction, recruitment and retention difficulties which are particularly difficult in the government sector as the salaries are not competitive with the real sector. As can be seen from the responses, states are aware of the HRM issues although no state responded that HRM was also one of the elements of risk management.

Five did not answer the question of attracting, recruiting and retaining personnel, while the other seven states have quite similar HRM measures in place. These seven did not respond to all the elements, but

[119] Johnason in Collings & Wood, 2009, pp. 19-37; Collings & Wood, 2009, pp. 1-16.
[120] Paauwe & Boon in Collings & Wood, 2009, pp. 38-54.

responded in part. All seven answered the question on attraction and recruitment and six out on retention (Chart 38).

Five states responded that they attract personnel by promoting the working environment (WE) and free education and training, three through educational institutions and social media (Inst. & SM), and one with an established system of financial and (military) social benefits (F & S ben.) or by motivation system of rewards and promotions (R & P). In addition, states recruit personnel based on the promotion of free education and training (E&T), a positive work environment (WE) and a system of remuneration and social benefits (R & S ben.), focusing on modern HRM trends. It is slightly different in the field of personnel retention as the emphasis is on free education and training and less on working environment, rewards and promotions, financial and social benefits and modern HRM, while only one state uses competitive salaries as a measure in place. Therefore, we can conclude that states apply similar measures the difference is only in the centre of gravity between the elements (Chart 38).

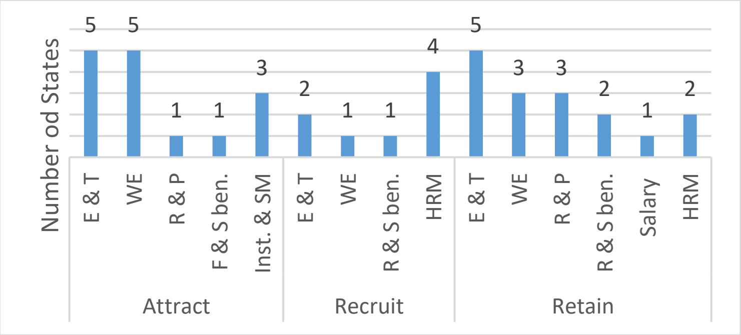


Chart 38: HMR states' System

3.4.1.1 Education, exercise and training

Education, exercise and training (EET) are integral parts of HRM as indirectly and directly correlated with employee performance and professional development and the development of the organisation. EET is also one of the key elements to attract and retain talented personnel within an organisation[121] and to increase the effectiveness and efficiency of the organisation's performance.[122] EET means building the capacity of the organisation and its operational capabilities. To improve the organisation's operational ability and capability, EET can be done via informal, non-formal and formal learning,[123] either within the organisation or by outsourcing or by national and international exercises.

An analysis was conducted focusing on EET within the organisation (in-house) outsourcing and national or international exercises. Answers to EET questions were obtained from 11 states surveyed. All 11 confirmed that they have a continuing professional plan in place. Nine answered that higher CD education and training for cyber staff is required, while two states do not have such a requirement. Ten stated that they have an education and training system in-house and five have a certification system for cyber competence (Chart 39). Responses to required hours of internal training varied, with four states not responding, one withholding this information and others responding that it depends on the course syllabus (from 120 hours up to 6 months).

[121] Heathfield, 2021, e-source.
[122] Islam, 2015, p. 1.
[123] Souto-Otero, 2021, p. 367.

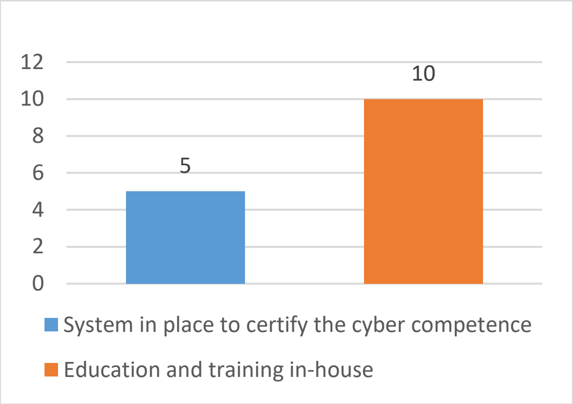


Chart 39: E & T in-house

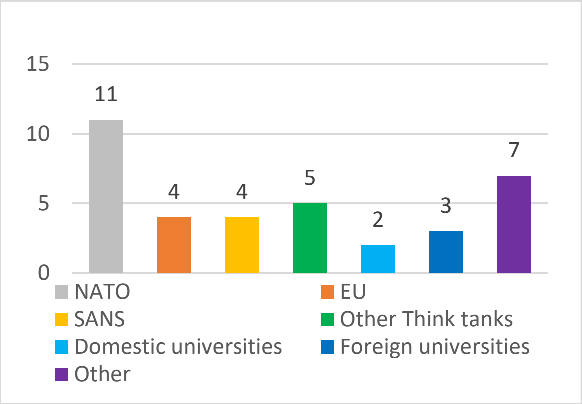


Chart 40: Outsourcing

Most of the states combine education and training in-house with national resources by sending cyber specialists to national or international educational institutions (e.g. forensics, malware analyst, computer engineering). Chart 40 shows that all 11 states use NATO educational capabilities (the NCI Academy, the NATO School Oberammergau, the Marshall Security Centre and CCDCOE) and four EU institutions (e.g. ENISA). They also use domestic and foreign universities (Baltic Defence College, European Security and Defence College, US Carnegie Melon University and US National Defence University) and think tank organisations. They use SANS, CompTIA, Microsoft, CISCO, Palo Alto and other national (commercial) think tanks and laboratories, which are not specifically mentioned by states.

Eight out of the 12 states surveyed annually participated in international cyber exercises at the strategic, operational and technical level, including on legal issues. Most of these exercises are conducted by NATO (including CCDCOE) such as Cyber Coalition, Locked Shields, Crossed Swords and NATO CMX (Chart 41). In addition to NATO exercises, countries also participate in EU exercises (Cyber Europe, EU Integrated Resolve) and participate in cyber exercises based on bilateral agreements.

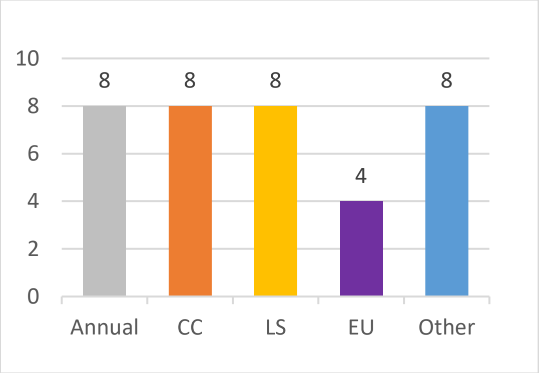


Chart 41: International Exercises

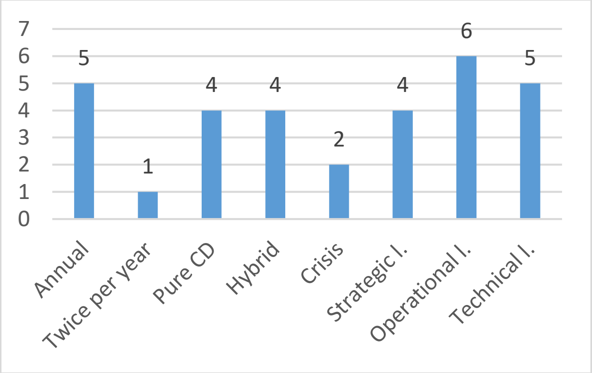


Chart 42: National Exercises

Regarding national cyber exercises, only six states out of the 12 answered that they have annual or biannual cyber exercises (Chart 42). Most include all three levels (strategic, operational and technical) and focus on pure CD and HT, while only two include a CD component.

3.5 Cooperation, collaboration and information sharing

Cooperation,[124] collaboration and information sharing are the cornerstones of the contemporary security environment. IE is no longer limited by physical borders as cyberspace is across domains as a medium for communication between subjects within it. In this regard, efficient CS (IS) is one of the key issues facing the world today as it serves as a pillar of a digitally resilient society.[125] The World Economic Forum stated that a single entity cannot have visibility over the entire problem space, therefore collaboration and information sharing are essential to cope with the contemporary threats.[126] A similar view is shared by Corall, Härma and Väljataga, who believe that the different approaches of states to national cyber or information security, their diverse digital capabilities and the interdependence of ICT call for an international dimension and international cooperation.[127] As a result, states should cooperate within international organisations and forums or engage in international cooperation based on bilateral agreements. At the same time, states should also comply with international standards and international law.

Information sharing serves as a platform for collective resilience and action by sharing strategic (type of threats, motivation and capability of threats and potential consequences), operational (decision-making, resource allocation, task prioritisation and tactics, techniques and procedures) and technical information (data typically derived from near real-time monitoring).[128] The same should be applied at the national level through public-private partnerships across CRI in cooperation and collaboration with industry and academia.

An analysis of cooperation, collaboration and information sharing was carried out at the national and international levels. Chart 43 shows that 12 states surveyed have very low collaboration and cooperation in IA and HT as only one state has it in place. Nine states implemented cooperation and collaboration in CS and CD, while on IS eight did. Ten had established national information sharing platforms (CSIRT network, intra-governmental network, cyber platform and others) and 11 use the Malware Information Sharing Platform (MISP). However, none provided any specific information.

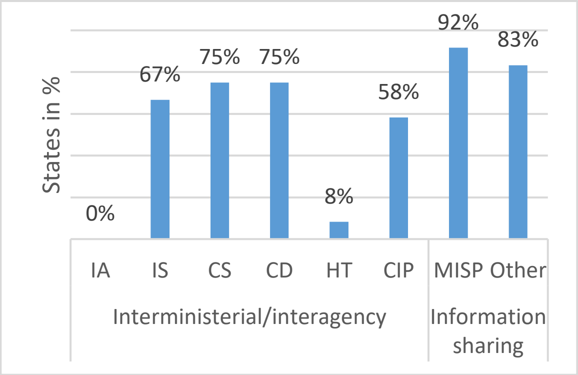


Chart 43: National Cooperation, Collaboration & Information Sharing

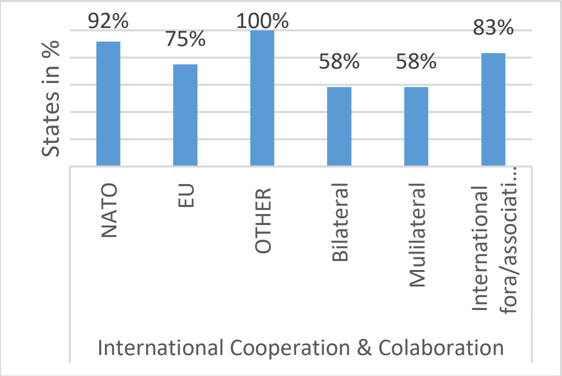


Chart 44: International Cooperation & Collaboration

States also confirmed collaboration and cooperation at the international level (Chart 44). Ten are members of international forums or associations (e.g. ITU, PESCO, etc.), and seven have concluded

[124] Cooperation: 'to work with other people by achieving one's own goals as part of a common goal'; Collaboration: 'to work together with somebody in order to achieve a single shared goal'. (Pantcheva, 2022, e-source).

[125] World Economic Forum, 2020, p. 4.

[126] Ibid, p. 5.

[127] Corall, Härma & Väljataga, 2018, p.

[128] World Economic Forum, 2020, pp. 6-7.

either bilateral or multilateral agreements or both. Additionally, 11 states exercised this collaboration within NATO, nine within the EU and all 12 with other international organisations such as the UN or OSCE.

States were also asked about cooperation and collaboration (C&C) with the private sector and academia (Chart 45). Most are active in both areas, with states not commenting in detail on the nature of the activity. From the responses, it could only be deduced that there was a collaboration with the private sector and academia in CD capability development or in general. The most common platform is via courses, exercises and projects sponsored by states.

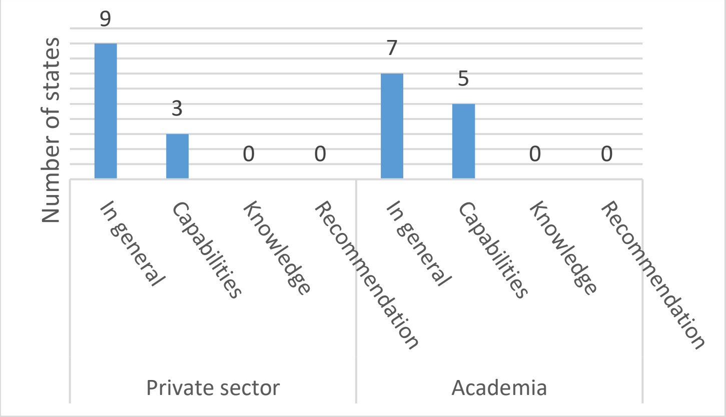


Chart 45: Cooperation & Collaboration on Development

As can be seen from Chart 46, cooperation, collaboration and information sharing is most developed at the international level. Ten states responded that they share information with international organisations and nine with other countries. Five of those states share technical information, two intel and four other information which were not specified. Eleven have established information sharing at the inter-agency or ministerial level. At this level, four share technical and intel information, while six states did not provide detailed information. Seven have information sharing at the public-private framework of cooperation, which is made by using MISP or another sharing platform. At the public-private framework, six states share technical information and one intel, while all seven share also other information which was not explained.

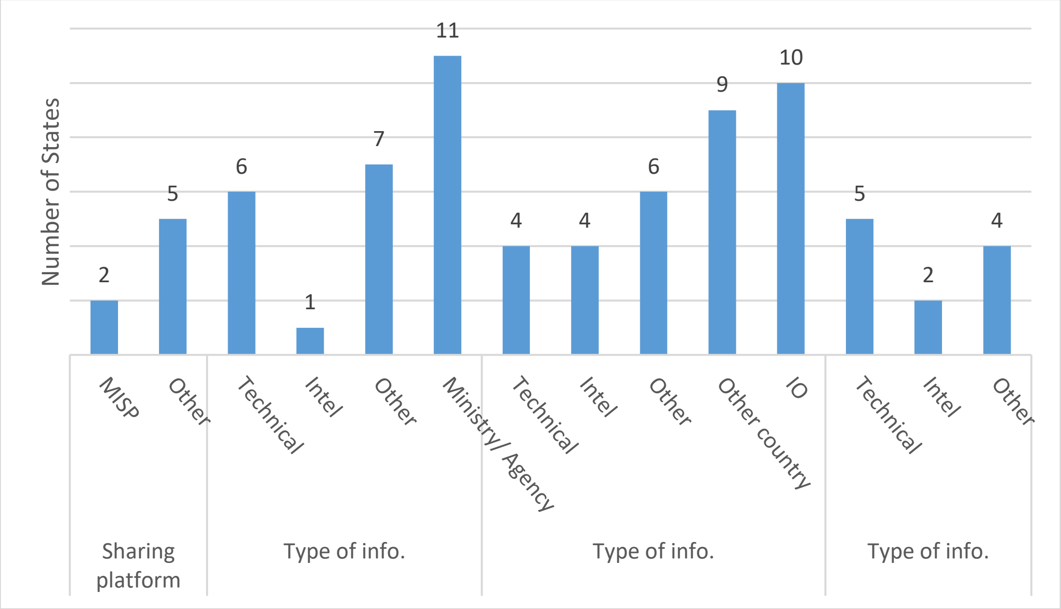


Chart 46: Information Sharing

4. Considerations and conclusions

Cyberspace and the IE have enabled real-time interactions between people and subjects of national and international law, while at the same time enabling the emergence of contemporary threats and challenges that are evolving at an incredible rate. The challenges are mainly reflected by the fact that information on cyber threats is not limited by physical boundaries and that they affect every entity within the IE. Therefore, it is necessary to establish mechanisms that will enable a joint response to such threats, for which it is necessary to have a common understanding of cyber-related terminology.

Although various terms such as CS, CR, HTs and operations are widely used, not all cyber-related definitions have been adopted by states and international organisations. Thus, we may have legitimate doubts about the mutual unified understanding of the cyber-related issues in the international community. As shown in Chart 47, only four states have adopted all cyber-related definitions and none of the international organisations has them all. The least accepted definitions are aggression (most states use the UN definition), IE and hybrid operations, followed by cyber operations (including CDO and CO), CR and cyberspace.

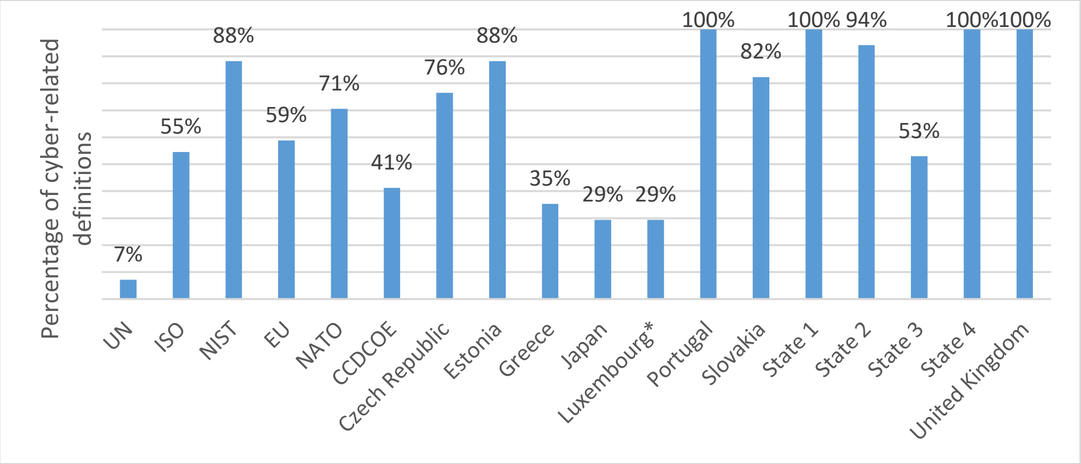
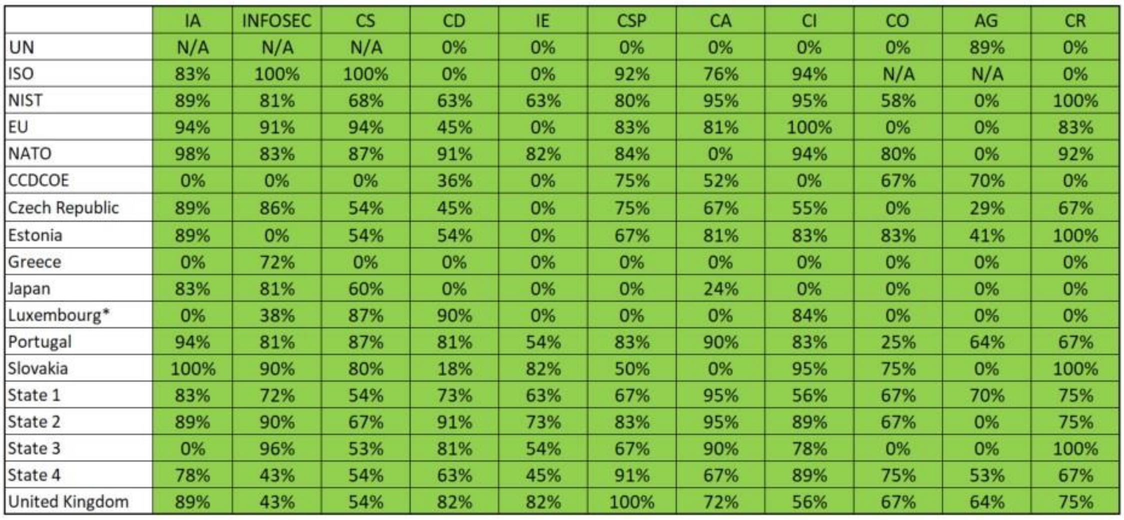


Chart 47: Cyber-related definitions accepted by states and international organisations

A definition can also be understood differently and depend on how many explicit elements are encompassed in a particular definition, on the type of the reader (civil, military or political) and whether the reader is a native or non-native speaker. The understanding of a definition is also related to the knowledge of basic terms, such as ICT, ICS, networks, etc. It is unnecessary to list an individual electronic system if an accepted term already exists and that is ICS. However, it is not appropriate to omit communication systems from definitions as today's technology is very difficult to divide into pure IT. Considering networks alone is not enough as networks can include both computer and communications nodes, so it was left to the reader how to evaluate this element. Some entities have an agnostic approach or so general a definition[129] that everyone understands it in their own way. However, our understanding of a given definition may not be the same as the understanding of the entity that developed the definition. The results in Figure 12 show just the authors' way of understanding an individual cyber-related concept and does not mean that states have poorer definitions. The biggest problem is that some states believe that there is no difference between IA and INFOSEC or that they prefer to use the term CS instead of INFOSEC or they considered data and information as synonyms. The concepts of INFOSEC and CS

[129] Definition should be general, however it should be clear enough, not allowing too much ambiguity, or it should be elaborated.

differ between NATO and the EU, and the latter advocates the concept of CS as a superset of INFOSEC, which is contrary to the generally accepted understanding of both.



	IA	INFOSEC	CS	CD	IE	CSP	CA	CI	CO	AG	CR
UN	N/A	N/A	N/A	0%	0%	0%	0%	0%	0%	89%	0%
ISO	83%	100%	100%	0%	0%	92%	76%	94%	N/A	N/A	0%
NIST	89%	81%	68%	63%	63%	80%	95%	95%	58%	0%	100%
EU	94%	91%	94%	45%	0%	83%	81%	100%	0%	0%	83%
NATO	98%	83%	87%	91%	82%	84%	0%	94%	80%	0%	92%
CCDCOE	0%	0%	0%	36%	0%	75%	52%	0%	67%	70%	0%
Czech Republic	89%	86%	54%	45%	0%	75%	67%	55%	0%	29%	67%
Estonia	89%	0%	54%	54%	0%	67%	81%	83%	83%	41%	100%
Greece	0%	72%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Japan	83%	81%	60%	0%	0%	0%	24%	0%	0%	0%	0%
Luxembourg*	0%	38%	87%	90%	0%	0%	0%	84%	0%	0%	0%
Portugal	94%	81%	87%	81%	54%	83%	90%	83%	25%	64%	67%
Slovakia	100%	90%	80%	18%	82%	50%	0%	95%	75%	0%	100%
State 1	83%	72%	54%	73%	63%	67%	95%	56%	67%	70%	75%
State 2	89%	90%	67%	91%	73%	83%	95%	89%	67%	0%	75%
State 3	0%	96%	53%	81%	54%	67%	90%	78%	0%	0%	100%
State 4	78%	43%	54%	63%	45%	91%	67%	89%	75%	53%	67%
United Kingdom	89%	43%	54%	82%	82%	100%	72%	56%	67%	64%	75%

Figure 12: Qualitative analysis of definition

Figure 12 shows that some entities have a 'N/A' designation, which means that we have evaluated that this definition does not apply to the evaluated entity. In certain categories, some states received a score of 0%. This was a result of the state having not yet adopted definitions at the national level, a universally accepted definition does not exist or widely accepted EU or NATO definitions are not the same.

All definitions have the same idea in general, but there is a lack of cohesiveness of the idea of an individual concept that would enable an effective unified response of the international community. A visualisation of the consistency of state's definitions with the organisations' definitions is drawn in Chart 48, which shows a large inconsistency of definitions between states and organisations. This overview of all definitions shows that only 3% of respondents verbatim used a concept fully coherent with the corresponding EU definition and 13% with the corresponding NATO definition and 44% of respondents chose their own definition regarding the concepts addressed, while 11 % have none definitions accepted.

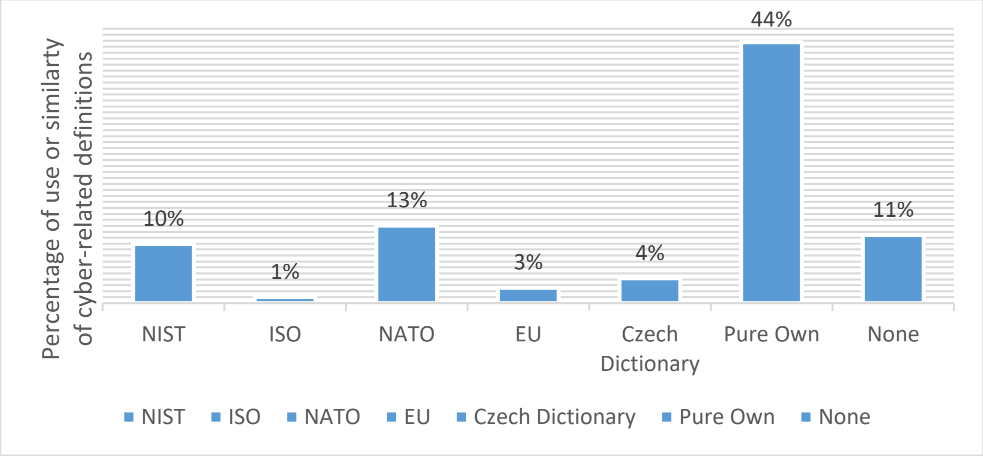


Chart 48: Use or similarity of states' definitions with organisations' definitions

Regarding NATO definitions, five states directly use the definition of COO and three of CDO. NATO has not yet adopted a definition of a cyber attack, therefore states have formulated their own definitions or perceptions of what a cyber attack is. This lack of cohesiveness does not only affect the common approach, but also the formation of international law and norms (e.g. Rules of Customary international law: state practice and opinion juris sive necessitates). Therefore, it would be necessary to unify the definitions as soon as possible, at least for cyberspace, CD, cyber attack,[130] CI[131], and cyber operation (including CDOs and COOs) and aggression. Unification of these terms would allow both states and international organisations to have a unified perception of the cyber threat, while at the same time having a common and unambiguous response or behaviour in cyberspace. This is particularly important today as most cyber attacks, incidents or operations target CRI, government institutions and the state economy aimed at destabilising the nation-state and consequently harming its residents. Therefore, every state, especially a NATO or EU member state, should understand at least the terms IE, cyberspace, CD, cyber attack, CI and cyber operation. States and international organisations or at least these two organisations should implement uniform measures at all levels and thus establish uniform rules of conduct and behaviour in IE and cyberspace as they would then comprehend and perceive the cyber threat uniformly.

An analysis of the legal and institutional framework has shown that states do not have a fully established legal framework in all areas of cyber-related concepts. In terms of the definitions and concepts covered by this study, most states have defined and implemented strategies for CS, followed by CD and CIP. The concept that is least covered is HT. Neither have states approached solutions comprehensively. According to the generic security architecture, the states have focused most on regulating the 'middle' of the security architecture, i.e. CS and CD, and not from the top to the bottom. This is most evident in the review of state strategies as only one state has an IA strategy and two have an INFOSEC strategy, while all twelve have a CS strategy. A strategy is a political idea, goal or concept of how a particular security issue should be addressed. It is the basis for the development of a particular field, including which entities need to be involved, established and developed. It must include indicators of development and individual phases leading to the final goal. Therefore, it is by no means sufficient to simply pass legislation, which is the basis for the legality of the operation of an entity, but these entities must also be developed to ensure their effective operation. They must develop internal policy, processes, procedures, knowledge and information management and operational frameworks to ensure the effective operational, technical and tactical implementation of high-level policy goals.

This is also reflected in the diversity between states of organisational frameworks for implementing cyber-related concepts. Of course, differences in the organisational framework are partly due to historical and cultural differences. Figure 13 shows that states have all four levels of security governance, but that the roles are divided between different government entities. Some have only one entity covering the full range of cyber-related concept tasks, while others have several different entities whose functions are divided into sub-tasks, e.g. IA concept: TEMPEST, crypto security, CIS security, personal security, etc. The same entities may have two roles as in the case of INFOSEC and CS governance, where the majority of states assigned these roles to the ministries responsible for the government's ICS or dedicated government bodies. We can ask whether such a concentration of different strategic roles and tasks within the same entity is effective. This question cannot be answered in this paper as the responses of the states were too general to understand how the internal organisational structure of each entity is implemented. The dual role of each entity also stems from the understanding of the cyber-related concept as some states reported that they do not see a difference between IA and INFOSEC or that they prefer to use the term CS rather than INFOSEC. Nevertheless, the importance of the NCSC and its embedded national CERT which serves as the central body for responding to cyber attacks at the operational level should be emphasised, especially if they are part of the intelligence service. In this way, the NCSC receives real-

[130] E.g.: "'Cyber attack is a deliberate and / or malicious act in / through cyberspace, which are reasonably expected to cause injury or death to persons or damage or harm or destruction to objects."' We hereby emphasize CA as an action that causes harm and damage to persons and objects, while also distinguishing between CA and cyber espionage.

[131] E.g.: "Cyber incident is any event, either natural or human made, generate in/via cyberspace, with malicious or non-malicious intent; deliberate, accidental or due to incompetence that compromise and threaten any of the components of the cyberspace or their functions."

time intelligence while providing technical intelligence to the intelligence service, which is in line with Klimburg's CS Framework Model.[132]

	Political/Strategic Level	Operational Level	Technical/Tactical Level
IA	NSA, NCSC, MoD, Institute for standardisation, National Accreditation Entity, National Entity for security of IS, Digital Office at the Presidency, Cabinet Office.	NSA, NCSC, IT Centre, Military Intelligence, ICS security Group, National Accreditation Entity, Personal Data protection Entity.	
INFOSEC	NSA, NCSC, Government Office, National Entity for security of IS, National INFOSEC Authority, Digital Office at the Presidency, Ministry for Economy, Ministry of Investment, Regional Development and Informatization, Ministry of Environmental Protection and Regional Development.	NCSC, IT Centre, Personal Data protection Entity, National CERT, National Radio and Television Centre, Other relevant ministries and bodies.	
CS	Government, Government Security Council, Cabinet Office, CS department at Ministry of Digitalisation, National Entity for security of IS, National INFOSEC Authority, National protection commissioner, Ministry for Economy, Ministry of Digital Governance, Ministry of transportation and Infrastructure, CS strategic entity.	NCSC, MoD, National Intelligence, Military Intelligence, National IT Security Council, Digital Security Supervisory Committee, ICT Agency, CS Council, CS board at Ministry of Communications, inter-ministerial committee, National Radio and Television Centre, CERTs, Other relevant ministries and bodies.	CERTs, MoD, NAF
CD	MoD, Military Intelligence, National INFOSEC Authority, Government Security Council, Defence Directorate at the Ministry of Foreign Affairs, National Entity for security of IS.	NCSC, MoD, Military Intelligence, NAF (Cyber Forces Command, Ncyber operationC /CDC), Council for CD, Council for CS, Cabinet Office / of Ministers, National INFOSEC Authority, Strategic Council for National Security, Ad hoc group (Police, Intelligence Service, NCSC and CDC), Inter-ministerial committee, Other relevant ministries and bodies.	NAF, National Guard/reserve, National Cyber Force, CERTs
HT	Government, National Security Council, National protection commissioner, Ministry of Foreign Affairs, MoD,	NCSC, Expert Group, Hybrid Operation Centre at Ministry of Interior, Defence Directorate at the Ministry of Foreign Affairs, National/Military Intelligence service, Other relevant ministries and bodies.	National Cyber Force
CIP	Entity responsible for Fire Rescue Service, National protection commissioner, National INFOSEC Authority, National entity for civil protection, Entity for CIP,	NCSC, National Intelligence, Military Intelligence, CD entity at NAF, CIP Centre, Ministry of Interior, Sectoral Ministries,	National CERT, CERTs

[132] Klimburg, 2012, p. 112.

	Ministry of transportation and Infrastructure, MoD, NAF.	Other relevant ministries and bodies.	

Figure 13: Organisational framework on Cyber-related concepts

The study did not determine whether the tasks of an individual entity correspond to its core tasks, which may affect the effectiveness of the implementation of tasks related to cyber-related concepts. However, like Klimburg, we found that some states have assigned a role of CS governance to entities whose basic tasks are not indirectly related to national security or ICS governance.[133] In this, it is more important which entities are subordinated (e.g. NCSC, national CERT or NCOC). However, it is completely different from the CD's operational framework as most of the assigned entities are already included in the national security system. As shown in Figure 14, some states have a CD operational framework at the government level and others at the level of ministries or government bodies. All entities that include NAF also have in common that the NCOC, CDC or Cyber Force Command that has direct command of MoD, Military Intelligence, CHOD or JFC, that is on a strategic or operational level.

Operational framework on CD	Working Level	Coordinating body for CS&CD
1. MoD 2. Military Intelligence 3. NAF (Cyber Forces Command, Ncyber operationC /CDC) 4. Council for CD 5. NCSC 6. Ministry of Digital Governance 7. Individual responsibility of each entity 8. Inter-ministerial committee 9. Council for CS 10. Ad hoc group (Police, Intelligence Service, NCSC and CDC) 11. Cabinet Office / of Ministers 12. National INFOSEC Authority 13. Strategic Council for National Security 14. Ministry of transportation and Infrastructure.	1. Ministry of Economy 2. Ministry of Digital Governance 3. Ministry of Foreign Affairs, 4. National INFOSEC Authority 5. National Accreditation Entity, 6. MoD 7. Individual responsibility of each entity 8. Ad Hoc Group (Police, Intelligence Service, NCSC and CDC) 9. Military Intelligence 10. NAF (Cyber Forces Command, Ncyber operationC /CDC) 11. NCSC 12. the Police 13. National CS Authority 14. National CERT 15. Other CERT/CSIRT authorities 16. Other relevant ministries and bodies.	Political/Strategic level: 1. NCSC 2. Ministry for Economy 3. Ministry of Digital Governance 4. Inter-ministerial committee 5. Ad hoc group (Police, Intelligence Service, NCSC and CDC) 6. CDC 7. Security board lead by MoD 8. National INFOSEC Authority 9. Cabinet Office / of Ministers 10. Strategic Council for National Security 11. Ministry of transportation and Infrastructure 12. Strategic Command at MoD Operational level: 1. J-6/ CD section at JFC 2. NCSC

Figure 14: Organisational framework on CD

In addition, most states have shared responsibility for CS and CD, however, they did not provide precise answers as to what shared responsibility really is and the role of the MoD and NAF in peacetime. Thus we cannot draw any conclusions on whether the coordination body for CS and CD at the operational level is well placed or not. However, we encourage states to consider the role of the MoD and NAF in the event of a hybrid attack or large-scale cyber attack and reconsider the suitability of a CS and CD coordinating body in civilian institutions at the operational level. In our view, this solution is sufficient in peacetime without a serious threat to national security, but it is ineffective in the event of a major cyber attack or a major hybrid threat.

[133] Klimburg, 2012, p. 112.

No state is resilient to a serious cyber attack or HT and therefore it would be probably the most effective to have an organisational structure similar to that for a natural disaster, where the MoD, including the NAF, assists civilian institutions on request and monitors the situation in the crisis response centre. The MoD and NAF are probably the only state institutions that carry out operational planning and operations and also cooperate and collaborate directly with the Allies in peacetime through various exercises and training in all domains of operations, from the strategic down to the technical level, including the legal component. NAFs must be interoperable with international organisations and Allies as CO can be kinetic or non-kinetic. However, it is quite understandable that each entity that uses a unique and separate ICS also has its own Network Security Operational Centre and CERT, which are responsible for CS and CD within the organisation. It is also important that the various CERTs are interconnected through platforms that allow real-time data exchange and, if necessary, joint action. CD is not only separated into passive and active CD, but can also be conducted as a DCO, hence a holistic and comprehensive approach should be taken. The national CD in peacetime should be ranked in stages, from CD within the organisation to shared national CD and in the form of cyber operation as the highest level of the national CD and the legal and institutional framework should be adapted accordingly.

To implement effective CS and CD, the proper cyber capabilities are needed; that is to say, a combination of personnel, technologies and organisational attributes. From the collected data, we found that states are building cyber capabilities primarily by investing in technology and knowledge. It is very positive that most states have an integrated in-house education system, while at the same time using training and exercises within NATO and the EU. Such a combination of knowledge acquisition is particularly important in terms of exchanging good practices and testing interoperability at national and international levels. It is also positive that most states use outsourcing and (commercial) think tank/laboratory organisations, but less than half of the states have a competency certification system in place. Some do not have offensive cyber capabilities or do not even intend to build them. Possession of offensive cyber capabilities does not affect the state's posture or does not mean that the state's posture is offensive. Offensive cyber capabilities allow the state to actively defend itself, while at the same time allowing it to better understand the attacker. The same is true in all other components of the military as states not only develop defence capabilities but are also offensive and they also train offensively, which does not mean that they will unnecessarily act offensively or pose a threat to international peace. Cyberspace, as one of the operational domains or as a cross-domain, is no different and so the same approach to ensuring national security is needed. Building cyber capabilities by upgrading ICT alone is not enough for effective CD. It is also necessary to build offensive cyber capabilities that will allow states to develop, among other things, tactical and technical procedures of CD that will stop an attacker from carrying out a cyber attack or operation. Therefore, it is not a question of whether an offensive cyber capability is needed, but how big and how trained it should be or, as Limnéll said, ‘cyber capabilities are essential for the nation-states and the armed forces that wish to be treated as credible actors’.[134]

The question of the operational and cost-effectiveness of the potential duplication of cyber capabilities at the national level (CS and CD operational and technical level), especially since all states face the same problem of personnel shortages is also important. It often happens that personnel from one state entity move to another due to better working conditions, salaries or benefits or else leave the state system and get a job in the private sector. The analysis showed that states have taken more or less the same measures in terms of employment and retention, among which education is probably the most attractive. However, education is a double-edged sword as it makes personnel attractive to the private sector, mainly because it is not necessary to invest time or money in already trained personnel. In any case, personnel outflow cannot be prevented, but it can be reduced among government bodies, especially if a uniform benefit and wage policy are in place.

Finally, this paper shows the level of states’ readiness to share information, which is also reflected in the quality of the data collected. We are aware that some information cannot be shared with the general

[134] Limnéll in Rantapelkonen & Salminen, 2013, p. 200.

public, but we believe that states could be more receptive to questions about the roles and responsibilities of each entity or on collaboration, cooperation and information sharing, especially with the private sector and academia.

Cyberspace is having an increasing effect on the contemporary security environment and if we want to be effective, we need to work together. Unlike the nuclear threat in which the consequences can be predicted fairly accurately, cyberspace does not allow this as the whole world is connected across all five spatial dimensions. Therefore, we can say that the level of common security does not depend on the strongest state, but on the weakest.

5. List of Charts and Figures

6. List of Tables

7. References

Actions, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/action, accessed on 25. 8. 2021.

Aggression, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/aggression, accessed on 25. 8. 2021

Allied Joint Doctrine for Information Operations, AJP 3.10, November 2009.

Allied Joint Doctrine for Communication and Information Systems, AJP-6, Ed. A, Ver. 1, NATO, Feb 2017.

Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, Edition A, version 1, NATO, January 2020.

Althonayan, A., & Andronache, A., 2018. Conference Paper: Shifting from Information Security towards a Cybersecurity Paradigm, September 2018, pp. 68-79.

Andress, J., & Winterfeld, S., 2014. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners (Second Edition), Elsevier: MA, USA.

An Introduction to the Cyber Threat Environment, 2018. Canadian Centre for Cyber Security, Government of Canada.

Approval of Terminology Proposals, AC/322-N(2019)0043-REV 1-AS1 (INV), NATO, 2020.

Bendovschi, A., 2015. 7th International Conference on Financial Criminology 2015, 13-14 April 2015, Wadham College, Oxford, United Kingdom: Cyber-Attacks – Trends, Patterns and Security Countermeasures, p. 24-31.

Barnes, I., A., 2018. Implementation of Active Cyber Defense Measures by Private Entities: The Need for an International Accord to Address Disputes, Monterey: Naval Postgraduate School.

Björck, F.; Henkel, M.; Stirna, J.; Zdravkovic, J., 2015. Cyber Resilience - Fundamentals for a Definition. Advances in Intelligent Systems and Computing, Vol. 353, New Contributions in Information Systems and Technologies, Vol. 1, Stockholm University, pp. 311–316.

Blair, Dennis C., Michael Chertoff, Frank J. Cilluffo, and Nuala O'Connor, eds., 2016. Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats. Washington, DC: George Washington University, Center for Cyber and Homeland Security.

Bodeau, D., & Graubart, R., 2013. Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment, url: https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf, accessed on 25. 8. 2021.

Brantly, A., & Smeets, M., 2020. Military Operations in Cyberspace, url: https://link.springer.com/content/pdf/10.1007/978-3-030-02866-4_19-1.pdf, accessed on 16. 9. 2021.

Brikše, I., 2006. The information environment: theoretical approaches and explanations, Informācijas vide Latvijā: 21. gadsimta sākums.: 2006. Url: https://www.szf.lu.lv/fileadmin/user_upload/szf_faili/Petnieciba/sppi/mediji/inta-brikse_anglu.pdf, accessed on 25. 8. 2021.

Broeders, D. 2021. Private active cyber defense and (international) cyber security—pushing the line?, Journal of Cybersecurity, 2021, Vol. 00, No. 0, pp. 1-14.

Brown, J., Data vs. Information vs. Insight, Benedictine University, url: https://online.ben.edu/programs/mba/resources/data-vs-information-vs-insight, accessed on 25. 8. 2021.

Cambridge International AS & A Level Information Technology, Cambridge International, url: https://www.cambridgeinternational.org/Images/285017-data-information-and-knowledge.pdf, accessed on 25. 8. 2021;

Capability, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/capability, accessed on 15. 1. 2022.

Capability, Cambridge Dictionary, Dictionary, url: https://dictionary.cambridge.org/dictionary/english/capability?q=capabilities, accessed on 15. 1. 2022.

Chaudhary, A.; Pundir, N.; Goel, G. 2013. Telecommunication Technologies, Advance in Electronic and Electric Engineering, Vol. 3, No. 3, Research India Publications, pp. 421-426.

Clark, D., 2010. Characterizing cyberspace: past, present and future. ECIR Working Paper, Massachusetts Institute of Technology, Cambridge: Massachusetts.

Collings, D. G., & Wood, G. 2009. Human resource management: A critical approach. In Collings, D. G., & Wood, G. (Eds.), Human resource management: A critical approach (pp. 1-16). London: Routledge.

Communication system, Definition, Webster dictionary, url: https://www.webster-dictionary.org/definition/communication%20system, accessed on 25. 8. 2021.

Communication Systems, Communication Technologies, Unit 3, p. 184 - 207, url: https://www.baschools.org/pages/uploaded_files/chap09.pdf, accessed on 17. 9. 2021.

Communication technology, Webster dictionary, Definition, url: https://www.webster-dictionary.org/definition/communications+technology, accessed on 16. 9. 2021.

Corall, T., Härma, K. & Väljataga, A., 2018. Enhancing international collaboration in cyber defence through national cyber security strategy development, Tallinn: CCDCOE.

COUNCIL DECISION 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information, EU, Official Journal of the European Union, L 274/5.

COUNCIL DIRECTIVE 2008/114/EC of 23 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, EU, Official Journal of the European Union, L 345/77.

Counter, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/counter, accessed on 25. 8. 2021.

Couretas, M., J., 2018. An Introduction to Cyber Modeling and Simulation. New York: John Wiley & Sons, Inc.

Craig, A. J. S., 2020. Capabilities and Conflict in the Cyber Domain An Empirical Study, United Kingdom: Cardiff University.

Creasey, J. & Glover, I., 2014. Cyber Security Incident Response Guide, Version 1, United Kingdom: CREST.

Cyber Primer, (2nd Edition), Ministry of Defence Shrivenham, July 2016,

Critical component, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/critical_component, accessed on 1. 7. 2021.

Critical Information Infrastructures, ENISA, url: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii, accessed on 14. 9. 2021.

Critical infrastructure, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/critical_infrastructure, accessed on 1. 7. 2021.

Cyber attack, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/Cyber_Attack, accessed on 1. 7. 2021.

Cyber attack, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/cyberattack, accessed on 25. 8. 2021.

Cyber attack, Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/cyberattack, accessed on 1. 7. 2021.

Cyberspace Capability, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/cyberspace_capability, accessed on 15. 1. 2022.

Cyber incident, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/cyber_incident, accessed on 1. 7. 2021.

Cyber Information Sharing: Building Collective Security, Insight Report, October 2020. World Economic Forum, url: https://www3.weforum.org/docs/WEF_Cyber_Information_Sharing_2020.pdf, accessed on 19. 1. 2022.

Cyber operations, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/cyberspace_operations, accessed on 1. 7. 2021.

Cyber operations, Old Dominion University, url: https://odu.edu/academics/programs/undergraduate/cyberoperations, accessed on 25. 8. 2021.

Cyber resiliency, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/cyber_resiliency, accessed on 1. 7. 2021.

Cybersecurity, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/cybersecurity, accessed on 1. 7. 2021.

Cybersafety, Merriam-Webster Dictionary, url: https://www.merriam-webster.com/dictionary/cybersafety, accessed on 25. 8. 2021.

Cyber Security Incident Management Guide, Centre for Cyber security Belgium, url: https://ccb.belgium.be/sites/default/files/cybersecurity-incident-management-guide-EN.pdf, accessed on 25. 8. 2021.

Cyberspace, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/cyberspace, accessed on 1. 7. 2021.

Cyber security event, BitLyth, What Is a Cybersecurity Event?, url: https://www.bitlyft.com/resources/cybersecurity-event-vs-incident-whats-the-difference, accessed on 25. 8. 2021.

Cyberthreat, Oxford dictionary, url: https://www.oxfordlearnersdictionaries.com/definition/english/cyberthreat, accessed on 25. 8. 2021.

Cyber threat, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/cyber_threat, accessed on 1. 7. 2021.

Cyberspace defence, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/cyberspace_defense, accessed on 1. 7. 2021.

Cyberspace, Definition, Webster dictionary, url: https://www.merriam-webster.com/dictionary/cyberspace, accessed on 1. 7. 2021.

Cyberspace, Definition, Cambridge dictionary, url: https://dictionary.cambridge.org/dictionary/english/cyberspace, accessed on 1. 7. 2021.

Da Silva, M., F., 2016. Cyber Security vs. Cyber Defense: A Portuguese view in the distinction. Cyberlaw: CIJIC.

Damage, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/damage, accessed on 25. 8. 2021.

Data, Definition, Webster dictionary, url: https://www.webster-dictionary.org/definition/data, accessed on 1. 7. 2021.

Data, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/data, accessed on 1. 7. 2021.

Defense, Merriam-Webster Dictionary, url: https://www.merriam-webster.com/dictionary/defense, accessed on 25. 8. 2021.

Defensive cyber operations, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/defensive_cyberspace_operations, accessed on 1. 7. 2021.

Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), UN, April 1974.

Definitions of offensive cyber capabilities, Australian Strategic Policy Institute, url: https://www.aspi.org.au/report/defining-offensive-cyber-capabilities, accessed on 15. 1. 2022.

Denning, E., D., 2013. Framework and Principles for Active Cyber Defense, Monterey: Naval Postgraduate School.

Do you know the difference between cyber security and information security?, 2018, IT Governance Blog, Published August 9, 2018, url: https://www.itgovernance.co.uk/blog/do-you-know-the-difference-between-cyber-security-and-information-security, accessed on 23. 11. 2021.

Dinstein, Y., Dahl, A., W., 2020. Oslo Manual on Select Topics of the Law of Armed Conflict, Rules and Commentary. Cham: Springer Nature Switzerland AG.

Dupont, B., 2019. The cyber-resilience of financial institutions: significance and applicability, Journal of Cybersecurity, Vol. 5, No. 1, 7 September 2019, pp. 1-17.

Elsaid, M., N., Oksaha, E., A., & Abdelghaly, A., A., 2013, Defining and Solving the Organizational Structure Problems to Improve the Performance of Ministry of State for Environmental Affairs – Egypt, International Journal of Scientific and Research Publications, Vo. 3, Issue 10, October 2013, pp. 1-10.

ENISA overview of cybersecurity and related terminology, Version 1, ENISA, September 2017, url: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, accessed on 1. 7. 2021.

Event, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/event, accessed on 1. 7. 2021.

Event, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/event, accessed on 25. 8. 2021.

Event, Simplicable, Security Events vs Security Incident, url: https://simplicable.com/new/security-event-vs-security-incident, accessed on 25. 8. 2021.

Falessi, N., Gavrila, R., Klejnstrup, M. R., & Moulinos, K., 2012. National Cyber Security Strategies. Practical Guide on Development and Execution. Heraklion: ENISA.

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018. NIST.

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, pp 201–206.

Galinec, D., Steingartner, W., 2017. 2017 IEEE 14th International Scientific Conference on Informatics: Combining cybersecurity and cyber defense to achieve cyber resilience, Informatics 2017, November 14-16, Poprad, Slovakia.

Galinec, D., 2018. Resilience is key. Per Concordiam, Volume 9, Issue 1, pp. 15-21.

Galinec, D., Možnik, D., & Guberina, B., 2017. Cybersecurity and cyber defence: national-level strategic approach, Automatika: Journal for Control, Measurement, Electronics, Computing and Communications, Volume 58, No. 3, p. 273-286.

Goel, S., Pon, D., & Menzies, J., 2006. Managing Information Security: Demystifying the Audit Process for Security Officers, Journal of Information System Security, Vol. 2, No. 2, 2006, pp. 25-45.

Greco, G., 2020. European Journal of Political Science Studies: Cyber Attacks as Aggression Crimes in Cyberspace in the Context of International Criminal Law, Vol. 4, Issue 1, pp. 40-47.

Harknett, R., J., & Smeets, M., 2020. Cyber campaigns and strategic outcomes, url: https://www.tandfonline.com/doi/pdf/10.1080/01402390.2020.1732354?needAccess=true/, accessed on 23. 11. 2021.

Hausken, K., 2020. Internet of Things: Cyber resilience in firms, organizations and societies, Elsevier, Vol. 11, September 2020, pp. 1-9.

Heathfield, S. M., 2021. What Is Human Resource Development?, url: https://www.thebalancecareers.com/what-is-human-resource-development-hrd-1918142, accessed on 18. 1. 2022.

Healey, J., 2019. The implications of persistent (and permanent) engagement in cyberspace, Journal of Cybersecurity, Vol. 5, No. 1, June 2019, pp. 1–15

High Level Taxonomy of Cyberspace Operations, IMSM-0222-2018, NATO.

Howard, J., D., & Longstaff, T., A., 1998. A Common Language for Computer Security Incidents; Sandia National Labs.: Livermore, CA, USA.

Hooda, S., 2019, Cloud Academy: Cybersecurity vs. Information Security: Is There a Difference?, Published September 26, 2019, url: https://cloudacademy.com/blog/cybersecurity-vs-information-security-is-there-a-difference/, accessed on 23. 11. 2021.

Hoffman, F., G., 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies.

IEEE Standard Glossary of Software Engineering Terminology, IEEE Std 610.12.-990, IEEE Standards Board, 1990.

IEEE Standard Glossary of Data Management Terminology, IEEE Std 610.5-1990, IEEE Standards Board, 1990.

IEEE Standard Glossary of Software Engineering Terminology, IEEE Std 610.10.1994, IEEE Standards Board, 1994.

Incident, BitLyth, What Is an Incident?, url: https://www.bitlyft.com/resources/cybersecurity-event-vs-incident-whats-the-difference, accessed on 25. 8. 2021.

Incident, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/incident, accessed on 25. 8. 2021..

Incident, Simplicable, Security Events vs Security Incident, url: https://simplicable.com/new/security-event-vs-security-incident, accessed on 25. 8. 2021.

Information, Definition, Webster dictionary, url: https://www.webster-dictionary.org/definition/Information, accessed on 25. 8. 2021.

Information, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/information, accessed on 1. 7. 2021.

Information assurance, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/information_assurance, accessed on 1. 7. 2021.

Information environment, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/information_environment, accessed on 1. 7. 2021.

Information operations, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/information_operations, accessed on 1. 7. 2021.

Information resources, Glossary, Computer Security Resource Center. NIST, url: https://csrc.nist.gov/glossary/term/information_resources, accessed on 1. 7. 2021.

Information security, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/information_security, accessed on 1. 7. 2021.

Information system, Definition, Webster dictionary, url: https://www.webster-dictionary.org/definition/information%20system, accessed on 25. 8. 2021.

Information system, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/information_system, accessed on 1. 7. 2021.

Information Systems vs. Information Technology, Florida tech, url: https://www.floridatechonline.com/blog/information-technology/information-systems-vs-information-technology/, accessed on 17. 9. 2021.

Information technology, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/information_technology, accessed on 16. 9. 2021.

Information technology, Definition, Webster dictionary, url: https://www.webster-dictionary.org/definition/information%20technology, accessed on 16. 9. 2021.

Information technology — Security techniques — Guidelines for cybersecurity, ISO/IEC 27032, First edition, ISO, 2012.

Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO/IEC 27000, Fifth ed., ISO, 2018.

Information Security Resources, SANS, https://www.sans.org/information-security/, accessed on 23. 1. 2021.

Information Security vs Cybersecurity: WHAT'S THE DIFFERENCE? City University of Seattle, Published November 22, 2019, url: https://www.cityu.edu/information-security-vs-cybersecurity/, accessed on 23. 11. 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, Czech Republic, National Cyber and Information Security Agency (NÚKIB), June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, Government of Estonia (the Ministry of Economic Affairs and Communication, the State Information Systems Authority, the Ministry of Defence), June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, Greece, Hellenic National Defence General Staff, June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, Japan, Government of Japan (Ministry of Defense), June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, Luxembourg, Ministry of Foreign and European Affairs, Directorate of Defence, June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, Portugal, Portuguese Armed Forces General Staff, June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, Slovak Republic, Military Intelligence, June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, State 1, National Armed Forces, June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, State 2, National Cyber Security Centre, June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, State 3, Information Security Administration, June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, State 4, National Armed Forces (NAF) Cyber Defence Command, June 2021.

Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, United Kingdom, Ministry of Defence, July 2021.

Institutional framework, OECD, url: https://stats.oecd.org/glossary/detail.asp?ID=6120, accessed on 22. 11. 2021.

International Humanitarian Law and Cyber Operations during Armed Conflicts, ICRC, November 2019.

International Law Applied to Operations in Cyberspace, MoD France, September 2019.

Intrusion, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/intrusion, accessed on 1. 7. 2021.

Islam, Z., 2015. Obligation of human resource management for retaining employees and increasing organizational performance: European Journal of Innovative Business Management, Vol. 2, 2015, 1-5.

Jirásek, P., Novák, L., Požár, J. 2013. Cyber security glossary. Praha: Policejni akademie ČR v Praze, Česká pobočka AFCEA.

Johnason, P., 2009. HRM in changing organizational contexts. In Collings, D. G. & Wood, G. (Eds.), Human resource management: A critical approach (pp. 19-37). London: Routledge.

Joint Publication 1, Doctrine for the Armed Forces of the United States, Chairman of the Joint Chiefs of Staff, 25 March 2013, Incorporating Change 1, 12 July 2017.

Joint Publication 3-12, Cyber Operations, Chairman of the Joint Chiefs of Staff, 8 June 2018.

Joint Publication 3-13, Information Operations, Chairman of the Joint Chiefs of Staff, 27 November 2012, Incorporating Change 1, 20 November 2014.

Joint Publication 6, Joint Communications System, Chairman of the Joint Chiefs of Staff, 10 June 2015, Incorporating Change 1, 04 October 2019.

Kello, L., 2013. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. – International Security, Vol. 38, No. 2, 7 – 40.

Kosseff, J., 2018. Defining Cybersecurity Law. Iowa Law Review: Vol. 103, No. 3, p. 985-1030.

Kott, A., & Linkov, I., 2019. Cyber Resilience of Systems and Networks, 1st ed, Cham: Springer International Publishing: Imprint: Springer.

Klimburg, A., 2012. National Cyber Security Framework Manual. Tallinn: NATO CCDCOE Publication.

Klump, R., 2018. Information Assurance vs. Cyber Security vs. Information Security: Clarifying the Differences, Lewis University: url: https://www.lewisu.edu/experts/wordpress/index.php/information-assurance-vs-cyber-security-vs-information-security-clarifying-the-differences/, accessed on 18. 11. 2021.

Knapp, J. K., 2009. Cyber Security and Global Information assurance: Threat Analysis and Response Solutions. New York: Information Science reference.

Lai, R. and Rahman, S. (Shawon), M., 2012. The International Journal of Multimedia & Its Applications, Analytic of China Cyberattack, Vol.4, No. 3, June 2012, pp. 37-56.

Laudon, C., Kenneth; Laudon, P., Jane, Glossary of terms, Essentials of Management Information Systems, 6e; Managing the Digital Firm; url: https://www.cs.csustan.edu/~lamie/cps603/glossary_of_terms.htm#I, accessed on 25. 8. 2021.

Legal framework, 2015, NRGI, https://www.resourcegovernance.org/sites/default/files/nrgi_Legal-Framework.pdf, accessed on 22. 11. 2021.

Le Gleut, R, Conway-Mouret, H, 2019. Information report No. 626. France: Working Group on European Defence.

Lee, M., R., 2015. White paper: The Sliding Scale of Cyber Security, SANS.

Lee, M., R. & Lee, R., 2016. White paper: The Who, What, Where, When, Why and How of Effective Threat Hunting, SANS.

Lin, H., S., 2010, Offensive Cyber Operations and the Use of Force, Journal of National Security Law & Policy, August 13, 2010, Vol. 4. No. 1, pp. 63-86.

MacLeod, A., 2015. Journal of Business Continuity & Emergency Planning: Effective information management and assurance for a modern organisation during a crisis, Vol.9, No. 2, May 2015, p. 52-59.

Maheshwari, R., & Agrawal, S., 2020. Strategic management, Agra-Mathura: SBPD Publishing House.

Mbanaso, U., M., & Dandaura, E., S., 2015. The Cyberspace: Redefining A New World, IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 17, Issue 3, Ver. VI (May – Jun. 2015), pp. 17-24.

Mendoza, A. J., 2017. Cyber Attacks and the Legal Justification for an Armed Response, Kansas: School of Advanced Military Studies, United States Army Command and General Staff College.

Military Balance 2015: Complex crises call for adaptable and durable capabilities, International Institute for Strategic Studies (IISS). Oxfordshire: Routledge for International Institute for Strategic Studies, p. 5-8.

Military Policy for Information Operations, MC 0422/6 (INV), NATO.

Miessler, D., The Difference Between Events, Alerts, and Incidents, url: https://danielmiessler.com/study/event-alert-incident, accessed on 25. 8. 2021.

Morris, J. L., Mazarr, J. M., Hornung, W. J., Pezard, S., Binnendijk, A., & Kepe, K., 2019. Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War, Santa Monica: RAND.

National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace, ENISA, May 2012.

NATO Glossary of Communication and Information Systems Terms and Definitions, AAP-31, Ed.: 3A, version 1, NATO, March 2005.

NATO Glossary of terms and definitions, AAP-06, Edition 2020, NATO, 2020.

NCI Agency, Who We Are, url: https://www.ia.nato.int/, accessed on 22. 11. 2021.

Network, Definition, Webster dictionary, url: https://www.webster-dictionary.org/definition/network, accessed on 25. 8. 2021.

Network, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/network, accessed on 1. 7. 2021.

Nohe, P., The Rise of Cyber Resilience, url: https://www.thesslstore.com/blog/the-rise-of-cyber-resilience/, accessed on 9. 9. 2021.

Occurrence, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/event, accessed on 25. 8. 2021.

Offensive cyberspace operations, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/offensive_cyberspace_operations, accessed on 1. 7. 2021.

Operation, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/operation, accessed on 25. 8. 2021.

Ophardt, A. J., 2010. Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow´s battlefield: DLTR, Vol. 9/1, pp. 1-27.

Orye, E., & Maennel, O., M., 2019. Recommendations for Enhancing the Results of Cyber Effects, url: https://ccdcoe.org/uploads/2019/06/Art_06_Recommendations-for-Enchasing-the-Results-of-Cyber-Effects.pdf, accessed on 1. 7. 2021.

Ottis, R., & Lorents, P., 2010. Cyberspace: Definition and Implications, 5th International Conference on Information Warfare and Security, Dayton, Ohio, USA, 08-09.04.2010, pp. 267-270.

Paauwe, J., & Boon, C. 2009. Strategic HRM: A critical review. In Collings, D. G., Wood, G. (Eds.) & Reid, M.A., Human resource management: A critical approach (pp. 38-54). London: Routledge.

Pantcheva, M., Collaborate or cooperate? url: https://site.uit.no/english/words/collaborate-or-cooperate/, accessed on 19. 1. 2022.

Phan, C., 2001. From Events to Incidents, SANS Institute.

Porche III, R., I., et al., 2013. Redefining Information Warfare Boundaries for an Army in a Wireless World. Sant Monica: RAND.

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

Preserve versus protect, Wikidiff, url: https://wikidiff.com/preserve/protect, accessed on 25. 8. 2021.

Preservation, Dictionary, Merriam-Webster, url: https://www.merriam-webster.com/dictionary/preservation, accessed on 25. 8. 2021.

Preservation versus protection, Wikidiff, url: https://wikidiff.com/preservation/protection, accessed on 25. 8. 2021.

Presidential Policy Directive 20, Executive Office of the President, 2012, url: https://irp.fas.org/offdocs/ppd/ppd-20.pdf, accessed on 25. 8. 2021.

Prevention, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/prevention, accessed on 25. 8. 2021.

Prevention versus protection, Wikidiff, url: https://wikidiff.com/prevention/protection, accessed on 25. 8. 2021.

Protection, Merriam-Webster Dictionary, url: https://www.merriam-webster.com/dictionary/protection, accessed on 25. 8. 2021.

Primary Directive on Information Management, C-M(2008)0113 (INV), NATO, 2008.

Probert, E., D., 2019. Organizational Structures & Incident Management for Cybersecurity in America, ITU: SlideShare, url: https://www.slideshare.net/DrDavidProbert/saltaworkshop1v12, accessed on 25. 8. 2021.

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities, COM(2020) 829 final, 2020/0365(COD), EU, 2020.

Rantapelkonen, J. & Salminen, M., 2013. The Fog of Cyber Defence, Helsinki: National Defence University.

Reid, R. & Van Niekerk, J., 2014. Conference paper on Information Security for South Africa: From information security to cyber security cultures, IEEE, pp. 1-7.

Response, Merriam-Webster Dictionary, url: https://www.merriam-webster.com/dictionary/response, accessed on 25. 8. 2021.

Rice, M.; Butts, J.; Shenoi, S.; 2011. International Journal Of Critical Infrastructure Protection: A signaling framework to deter aggression in cyberspace, Elsevier, Vol. 4, March 2011, pp. 57-65.

Rid, Th., 2013. Cyber War Will Not Take Place. Oxford: New York.

Rõigas H., & Jermalavičius, T., 2021. So Far, Yet So Close: Japanese and Estonian Cybersecurity Policy

Perspectives and Cooperation, ICDS: Estonia.

Ruffle, S.; Coburn, A.; Ralph, D.; Bowman, G.; 2013. Cambridge Risk Framework. Profile of a Macro-Catastrophe Threat Type: Cyber Catastrophe, Cambridge: Cambridge Centre for Risk Studies.

Safety versus security, Wikidiff, url: https://wikidiff.com/safety/security, accessed on 25. 8. 2021.

Safety, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/safety, accessed on 25. 8. 2021.Secure versus safe; Wikidiff, url: https://wikidiff.com/secure/safe, accessed on 25. 8. 2021.

Sander, B., 2019. 2019 11th International Conference on Cyber Conflict: The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations, NATO CCD COE Publications, Tallinn, pp. 361-381.

Security, Merriam-Webster Dictionary, url: https://www.merriam-webster.com/dictionary/security, accessed on 25. 8. 2021.

Security Audit, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/security_audit, accessed on 1. 7. 2021.

Security relevant event, Glossary, Computer Security Resource Center, NIST, url: https://csrc.nist.gov/glossary/term/security_relevant_event, accessed on 1. 7. 2021.

Schatz, D., Bashroush, R., Wall, J., 2017. Journal of Digital Forensics, Security and Law: Towards a More Representative Definition of Cyber Security, Volume 12, No. 2, Florida: Embry-Riddle Aeronautic University, pp 53–74.

Scheerder, T., 2012. Threat Perception Politics: A Comparative Case Study into Difference in Threat Perception between Terrorism and Climate Change in United States, Netherlands: Radboud University Nijmegen.

Schou, C. & Hernandez, S., 2015. Information Assurance Handbook: Effective Computer Security and Risk Management Strategies, Published by McGraw-Hill Education.

Schwartz, M., Bennett, W. R., & Stein, S. 1996. Communication systems and techniques. IEEE: Press New York.

Solms, von R., Van Niekerk, J., 2013. Computers & Security: From information security to cyber security, No. 38, 2013, pp. 97-102.

Sommer, F., Dürrwang, J., Kriesten, R., 2019. Survey and Classification of Automotive Security Attacks, MDPI Journals; Information, Vol. 10, No. 4, Sec. 148, April 2019, 10, pp. 1-29.

Sosin, A., 2018. How to increase the information assurance in the information age, Journal of Defense Resources Management, Vol. 9, Issue 1, pp. 45-57.

Souto-Otero, M., 2021. Validation of non-formal and informal learning in formal education: Covert and overt. European Journal of Education, Vol. 56, Issue 3, 365– 379.

Standard, Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/standard, accessed on 25. 8. 2021.

Štrucl D., 2020. Contemporary Military Challenges: Terminology confusion in ensuring cyberspace security, Vol.22, No. 4, October 2020, pp. 31-47.

Tallinn manual 2.0 on the international law applicable to cyber operations, Second edition, CCDCOE, 2017.

The Cyber Resilience Blueprint: A New Perspective on Security, Symantec, url: https://www.ten-inc.com/presentations/Symantec-The-Cyber-Resilience-Blueprint.pdf, accessed on 9. 9. 2021.

The Global Information Environment, FM 100-6, Information Operations, Headquarters, Department of the Army, 27 August 1996.

Tuovinen, J., & Frilander, K., 2019. Militarizing Red Teaming – Agile And Scalable Process For Cyber Red Teaming Using Adaptive Planning And Execution Framework, University of Jyväskylä.

Traynor, I., 2007. Russia accused of unleashing cyberwar to disable Estonia, url: https://www.theguardian.com/world/2007/may/17/topstories3.russia, accessed on 23. 11. 2021.

Understanding difference between Cyber Security & Information Security, 2016, CISO Platform, Published, July 21, 2016, url: https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information, accessed on 23. 11. 2021.

Valeriano, B. Maness, R. C., 2015. Cyber War versus Cyber Realities: Cyber Conflict in the International System. New York: Oxford University Press.

Yuchen, H., DAI 532 Applied Digital Electronics, San Francisco State University, San Francisco, url: https://www.coursehero.com/file/83145687/CHAPTER-1-INRODUCTION-TO-DIGITAL-COMMUNICATION-SYSTEMSpdf/, accessed on 25. 8. 2021.

What is cyber resilience?, ECB, url: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html, accessed on 25. 8. 2021.

Wither, K. J., 'Defining Hybrid Warfare,' per Concordiam: Journal of European Security Defense Issues 10, No. 1, 2020: p. 7-9.

8. Abbreviations

AG	Aggression
C&C&InfSh	Cooperation, collaboration and information sharing
C&C	Cooperation and Collaboration
CCDCOE	Cooperative Center of Excellence for Cyber Defence
CD	Cyber Defence
CDC	Cyber Defence Centre
CDO	Cyber Defensive Operation
CI	Cyber Incident
CIP	Critical Infrastructure Protection
CIS	Communication and Information System
CIS CIP	Communication and Information System Critical Infrastructure Protection
CO	Cyber Operations
COO	Cyber Offensive Operation
CR	Cyber Resilience
CRI	Critical Infrastructure
CS	Cyber Security
CSP	Cyberspace
DODIN	Department of Defence information network
EET	Education, Exercise and Training
ENISA	European Union Agency for Cybersecurity
EU	European Union
HO	Hybrid Operation
HRM	Human Resource Management
IA	Information Assurance
ICRC	International Committee of the Red Cross
IE	Information Environment
IEEE	Institute of Electrical and Electronics Engineers
IHL	International Humanitarian Law
ICT	Information Communication Technology
IO	Information Operations
INFOSEC	Information Security
IS	Information System
ISMS	Information Security Management System

the ISO	International Organisation for Standardisation
MoD	Ministry of Defence
NAF	National Armed Forces
NATO	North Atlantic Treaty Organisation
NCF	National Cyber Force
NCIE	National Cyber and Information Security Entity
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Authority
UN	United Nations

9. Appendix 1: Rudimentary definition

9.1 Information system

ISO	Set of applications, services, information technology[135] assets, or other information-handling components.[136]
NIST 1	A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (Note: Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems) [137]
NIST 2	An interconnected set of information resources[138] under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.[139]
NIST 3	A computer-based system used by an issuer to perform the functions necessary for PIV Card or Derived PIV Credential issuance as per (FIPS 201-2). [140]
Cyber security glossary	1) A functional aggregate enabling goal-oriented and systematic acquisition, processing, storage and access to information and data. Includes data and information sources, mediums, hardware, software and utilities, technologies and procedures, related standards and employees; (2) A complex of elements existing in mutual interaction (L. von Bertallanfy, 1956). [141]
Glossary of terms	Interrelated components working together to collect, process, store, and disseminate information to support decision making, coordination, control, analysis, and visualization in an organization. [142]
Webster dictionary	System consisting of the network of all communication channels used within an organization.[143]

[135] Information technology and information system are often used interchangeably or considered as synonymous. Information system consists of people, processes, and information technology to process and move information. Therefore, information technology is a subset of information system. Florida tech, Information Systems vs. Information Technology, url: https://www.floridatechonline.com/blog/information-technology/information-systems-vs-information-technology/, accessed on 17. 9. 2021.

[136] ISO/IEC 27000, Fifth edition, 2018.

[137] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/information_system, accessed on 1. 7. 2021.

[138] Definition of information resources: Information and related resources, such as personnel, equipment, funds, and information technology. NIST, url: https://csrc.nist.gov/glossary/term/information_resources accessed on 1. 7. 2021.

[139] Ibid.

[140] Ibid.

[141] Jirásek P., Novák L., Požár J., 2013.

[142] Laudon, C., Kenneth; Laudon, P., Jane, Glossary of terms, Essentials of Management Information Systems, 6e; Managing the Digital Firm; url: https://www.cs.csustan.edu/~lamie/cps603/glossary_of_terms.htm#I, accessed on 25. 8. 2021.

[143] Webster dictionary, Definition, Information system, url: https://www.webster-dictionary.org/definition/information%20system, accessed on 25. 8. 2021.

IEEE	A data processing system integrated with such other process as office automation and data communication.[144] A mechanism used for acquiring, filing, storing, and retrieving and organized body of knowledge.[145]

9.2 Information technology

NIST 1	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.[146]
NIST 2	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources.[147]
NIST 3	Computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data. IT components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware and software. [148]
NIST 4	The art and applied sciences that deal with data and information. Examples are capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage, and retrieval of data and information. [149]
Webster dictionary	Applied computer systems - both hardware and software, and often including networking and telecommunications, usually in the context of a business or other enterprise. Often the name of the part of an enterprise that deals with all things electronic. [150]

[144] IEEE Std 610.10-1994, 1994.

[145] IEEE Std 610.5-1990, 1990.

[146] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/information_technology, accessed on 16. 9. 2021.

[147] Ibid.

[148] Ibid.

[149] Ibid.

[150] Webster dictionary, Definition, Information technology, url: https://www.webster-dictionary.org/definition/information%20technology, accessed on 16. 9. 2021.

9.3 Communication system[151]

NIST 1	A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (Note: Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems) [152]
NIST 2	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.[153]
NIST 3	A computer-based system used by an issuer to perform the functions necessary for PIV Card or Derived PIV Credential issuance as per (FIPS 201-2). [154]
Cyber security glossary	System which provides for the transfer of information among end users. It includes end communication devices, transfer environment, system administration, handling by personnel and operational conditions and procedures. It may also include means of cryptographic protection. [155]
Glossary of terms	Telecommunications system: A collection of compatible hardware and software arranged to communicate information from one location to another.[156]
Webster dictionary	A system or facility capable of providing information transfer between persons and equipment. The system usually consists of a collection of individual communication networks, transmission systems, relay stations, tributary stations, and terminal equipment capable of interconnection and interoperation so as to form an integrated whole. These individual components must serve a common purpose, be technically compatible, employ common procedures, respond to some form of control, and generally operate in unison. (Communications Standard Dictionary, 2nd Edition, Martin H. Weik).[157]

[151] Communication technology and communication system are not considered as synonymous. While communication system is consist of various systems, networks, media, hardware, protocols, and software, is the communications technology an activity of designing and constructing and maintaining communication systems (Webster dictionary, Definition, Communication technology, url: https://www.webster-dictionary.org/definition/communications+technology, accessed on 16. 9. 2021).
Communication technology is the transfer of messages (information) among people and/or machines through the use of the technology (Communication Systems, Communication Technologies, Unit 3, p. 188, url: https://www.baschools.org/pages/uploaded_files/chap09.pdf, accessed on 17. 9. 2021.).
Telecommunication is any type of communication (transmission, emission or reception of information) by usage various electrical and electromagnetic technologies: wire, optical, radio, telephone, satellite, or other electromagnetic systems, and the Internet (Chaudhary et al, 2013, p. 421-422).

[152] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/information_system, accessed on 1. 7. 2021.

[153] Ibid.

[154] Ibid.

[155] Jirásek P., Novák L., Požár J., 2013.

[156] Laudon, C., Kenneth; Laudon, P., Jane, Glossary of terms, Essentials of Management Information Systems, 6e; Managing the Digital Firm; url: https://www.cs.csustan.edu/~lamie/cps603/glossary_of_terms.htm#I, accessed on 25. 8. 2021.

[157] Webster dictionary, Definition, Communication system, url: https://www.webster-dictionary.org/definition/communication%20system, accessed on 25. 8. 2021.

IEEE	A communications system or communication system is a collection of individual telecommunications (communications) networks, transmission systems, relay stations, tributary stations, and (data) terminal equipment usually capable of interconnection and interoperation to form an integrated whole. The components of a communications system serve a common purpose, are technically compatible, use common procedures, respond to controls, and operate in union.[158]

9.4 Network

NIST 1	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.[159]
NIST 2	An open communications medium, typically the Internet, used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the network's security; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking) and passive (e.g., eavesdropping) attack at any point between the parties (e.g., claimant, verifier, CSP, RP).[160]
NIST 3	A system implemented with a collection of connected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.[161]
Webster dictionary	Set of computer terminals (workstations) and servers which are mutually interconnected in order to exchange data and communicate. [162]
Webster dictionary	Hardware and software data communication systems. The OSI seven layer model attempts to provide a way of partitioning any computer network into independent modules from the lowest (physical) layer to the highest (application) layer. Many different specifications exist at each of these layers. Networks are often also classified according to their geographical extent: local area network (LAN), metropolitan area network (MAN), wide area network (WAN) and also according to the protocols used. (Tanenbaum, A., "Computer Networks; 2nd ed.", Prentice Hall, Englewood Cliffs, NJ, 1989.).[163]
IEEE	An arrangement of components, or nodes, and interconnecting branches.[164]

[158] Schwartz, M., Bennett, W. R., & Stein, S., 1996; Yuchen, H., DAI 532 Applied Digital Electronics, url: https://www.coursehero.com/file/83145687/CHAPTER-1-INRODUCTION-TO-DIGITAL-COMMUNICATION-SYSTEMSpdf/, accessed on 25. 8. 2021.

[159] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/network, accessed on 1. 7. 2021.

[160] Ibid.

[161] Ibid.

[162] Webster dictionary, Definition, Network, url: https://www.webster-dictionary.org/definition/network, accessed on 25. 8. 2021.

[163] Webster dictionary, Definition, Network, url: https://www.webster-dictionary.org/definition/network, accessed on 25. 8. 2021.

[164] IEEE Std 610.10-1994, 1994.

9.5 Data

NIST 1	Information in a specific representation, usually as a sequence of symbols that have meaning.[165]
NIST 2	A variable-length string of zero or more (eight-bit) bytes.[166]
NIST 3	Distinct pieces of digital information that have been formatted in a specific way.[167]
NIST 4	Pieces of information from which “understandable information” is derived. [168]
NIST 5	A subset of information in an electronic format that allows it to be retrieved or transmitted. [169]
NIST 6	A representation of information as stored or transmitted. [170]
NIST 7	Any piece of information suitable for use in a computer. [171]
NIST 8	A representation of information, including digital and non-digital formats. [172]
Glossary of terms	Streams of raw facts representing events occurring in organizations or the physical environment before they have been organized and arranged into a form that people can understand and use.[173]
Webster dictionary	Numbers, characters, images, or other method of recording, in a form which can be assessed by a human or (especially) input into a computer, stored and processed there, or transmitted on some digital channel. Computers nearly always represent data in binary. Data on its own has no meaning, only when interpreted by some kind of data processing system does it take on meaning and become information. People or computers can find patterns in data to perceive information, and information can be used to enhance knowledge. Since knowledge is prerequisite to wisdom, we always want more data and information. But, as modern societies verge on information overload, we especially need better ways to find patterns.[174]

[165] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/data, accessed on 1. 7. 2021.

[166] Ibid.

[167] Ibid.

[168] Ibid.

[169] Ibid.

[170] Ibid.

[171] Ibid.

[172] Ibid.

[173] Laudon, C., Kenneth; Laudon, P., Jane, Glossary of terms, Essentials of Management Information Systems, 6e; Managing the Digital Firm; url: https://www.cs.csustan.edu/~lamie/cps603/glossary_of_terms.htm#I, accessed on 25. 8. 2021.

[174] Webster dictionary, Definition, Data, url: https://www.webster-dictionary.org/definition/communication%20system, accessed on 25. 8. 2021.

Benedictine University	Data is the raw numbers that we capture according to some agreed to standards.[175]
Cambridge International	Data consists of raw facts and figures. D ata refers to raw input that when processed or arranged makes meaningful output.[176]
IEEE	A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means.[177]

9.6 Information

NIST 1	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. An instance of an information type.[178]
NIST 2	1. Facts and ideas, which can be represented (encoded) as various forms of data. 2. Knowledge—e.g., data, instructions—in any medium or form that can be communicated between system entities.[179]
NIST 3	1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.[180]
NIST 4	Meaningful interpretation or expression of data. [181]
NIST 5	Data that has semantic content (i.e. meaning) in a certain context. [182]
Cyber security glossary	Any sign expression which makes sense for the communicator and receiver. [183]
Glossary of terms	Data that have been shaped into a form that is meaningful and useful to human beings.[184]

[175] Brown, J. Data vs. Information vs. Insight, Benedictine University, url: https://online.ben.edu/programs/mba/resources/data-vs-information-vs-insight, accessed on 25. 8. 2021.

[176] Cambridge International, Cambridge International AS & A Level Information Technology, url: https://www.cambridgeinternational.org/Images/285017-data-information-and-knowledge.pdf, accessed on 25. 8. 2021.

[177] IEEE Std 610.12-1990, 1990; IEEE Std 610.10-1994, 1994.

[178] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/information, accessed on 1. 7. 2021.

[179] Ibid.

[180] Ibid.

[181] Ibid.

[182] Ibid.

[183] Jirásek P., Novák L., Požár J., 2013.

[184] Laudon, C., Kenneth; Laudon, P., Jane, Glossary of terms, Essentials of Management Information Systems, 6e; Managing the Digital Firm; url: https://www.cs.csustan.edu/~lamie/cps603/glossary_of_terms.htm#I, accessed on 25. 8. 2021.

Webster dictionary	A collection of facts from which conclusions may be drawn. Any fact or set of facts, knowledge, news, or advice, whether communicated by others or obtained by personal study and investigation; any datum that reduces uncertainty about the state of any part of the world; intelligence; knowledge derived from reading, observation, or instruction.[185]
Benedictine University	Information is a collection of data points that we can use to understand something about the thing being measured.[186]
Cambridge International	Information is data that has meaning. Data + Meaning = Information.[187]

9.7 Cyber Threat

NIST 1	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[188]
NIST 2	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[189]
NIST 3	An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss. Note: The specific causes of asset loss, and for which the consequences of asset loss are assessed, can arise from a variety of conditions and events related to adversity, typically referred to as disruptions, hazards, or threats. Regardless of the specific term used, the basis of asset loss constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions.[190]
NIST 4	Potential cause of an unwanted incident, which may result in harm to a system or organization. [191]

[185] Webster dictionary, Definition, Information, url: https://www.webster-dictionary.org/definition/Information, accessed on 25. 8. 2021.

[186] Brown, J. Data vs. Information vs. Insight, Benedictine University, url: https://online.ben.edu/programs/mba/resources/data-vs-information-vs-insight, accessed on 25. 8. 2021.

[187] Cambridge International, Cambridge International AS & A Level Information Technology, url: https://www.cambridgeinternational.org/Images/285017-data-information-and-knowledge.pdf, accessed on 25. 8. 2021.

[188] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/cyber_threat, accessed on 1. 7. 2021.

[189] Ibid.

[190] Ibid.

[191] Ibid.

Canadian Centre for Cyber security	A cyber threat is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains. [192]
University of Cambridge	Cyber threats cover a wide range of malicious activity that can occur through cyberspace. Such threats include web site defacement, espionage, theft of intellectual property, denial of service attacks, and destructive malware.[193]
Oxford dictionary	The possibility that somebody will try to damage or destroy a computer network, computer system or website by secretly changing information on it without permission.[194]

[192] Canadian Centre for Cyber security, 2021, p. 2.

[193] Ruffle, et al., 2013, p. 4.

[194] Oxford dictionary, Definition, Cyberthreat, url: https://www.oxfordlearnersdictionaries.com/definition/english/cyberthreat, accessed on 25. 8. 2021.

10. Appendix 2: Questionnaire A: Terminology

10.1 Information assurance

UN	N/A
ISO	Does not use Information assurance but Risk management: *"coordinated activities to direct and control an organization with regard to risk. Risk management process systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk."* [195]
NIST	*"Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Note: DoDI 8500.01 has transitioned from the term information assurance (IA) to the term cybersecurity. This could potentially impact IA related terms."* [196]
EU	*"Information assurance in the field of communication and information systems is defined as the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective information assurance must ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity."*[197]
NATO 1	*"Information assurance is the protection and defense of information and information systems by ensuring their availability, integrity, and confidentiality. Information assurance includes elements of physical security (e.g., personnel and document security) and information security. Information assurance is represented as consisting of five elements of security: personnel security, physical security, security of information, CIS security (includes cyber defence), and industrial security. (CIS security is an element of information assurance, and consists of the application of security measures for the protection of communication, information, and other electronic systems; and the information that is stored, processed, or transmitted in these systems with respect to availability, integrity, authentication, confidentiality, and non-repudiation. It includes defensive measures to counter cyber attacks and mitigate their effects, preventive CIS security measures, and user awareness as cyber defence)."* [198]
NATO 2	*"The principle of Information Assurance is described as the set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, nonelectronic systems, and the information that is stored, processed or transmitted in these systems with*

[195] ISO/IEC 27000, Fifth edition, 2018.

[196] Ibid.

[197] Official Journal of the European Union, L 274/5.

[198] NATO, AJP-6, Ed. A, Ver. 1, Feb 2017.

	respect to confidentiality, integrity, availability, non-repudiation and authentication." [199]
CCDCOE	*NONE*
Czech Republic	Provided definition from The Cyber Security Glossary:[200] *"A set of measures to achieve the required level of confidence in the protection of communication, information and other electronic as well non-electronic systems and information stored, processed or transferred in these systems with regard to confidentiality, integrity, availability, undeniability and authenticity."* [201] *"The Czech Republic does not see a difference between the terms Information Security and Information Assurance."* [202]
Estonia*	*"Information assurance in the field of communication and information systems is defined as the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users."* [203]
Greece	*Not officially defined yet.* [204]
Japan	*The term "Information assurance" is not defined by national law and its universally accepted definition does not exist. In case of MOD/SDF, the term is defined as follows:* *"Maintaining confidentiality (making sure that access to digital data is limited only to users with permission to access to the data), integrity (securing and protecting the status that digital data and its processing are accurate and complete), availability (making sure that users with permission to access to digital data can access to the data whenever necessary), identification and authentication (making sure that genuineness of identities of users and components of information systems can be confirmed) and nonrepudiation (making sure that users who sent or received digital data via information systems cannot deny the fact) of information systems and their data. (The Information Assurance Directive 2(2))."*[205]
Luxembourg*	*NONE. "In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case). "* [206]
Portugal	*"A set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, nonelectronic systems, and information that is stored, processed or transmitted in these*

[199] NATO, Primary Directive on Information Management (C-M(2008)0113 (INV)).

[200] Jirásek P., Novák L., Požár J., 2013.

[201] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[202] Ibid.

[203] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[204] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[205] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[206] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

	systems with respect to confidentiality, integrity, availability, non-repudiation and authentication." [207]
Slovakia	*Uses NATO accepted definition.* [208]
State 1	*"There is not approved definition of Information Assurance. The NAF consider all procedures that are required to ensure Availability, Integrity, Confidentiality, Authentication and Nonrepudiation principles of data and information systems, including risk assessment and business continuity planning."* [209]
State 2	*"Measures that protect and defend information and information systems by ensuring their availability, integrity, authentications, confidentiality and non-reputation. These measures include providing for restoration of information systems by incorporating protection, detection and reaction capabilities."* [210]
State 3	*NONE* [211]
State 4	*"Ensuring the CIA (Confidentiality, Integrity, and Availability) of the information, as well as the non-repudiation."* [212]
United Kingdom	*"The confidence that the information within the Defence community is maintained reliably, accurately, securely and is available when required."* [213]

10.2 Information security

UN	N/A
ISO	*"Information security: preservation*[214] *of confidentiality, integrity and availability of information (NOTE: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved)."* [215]
NIST	*"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."* [216]
EU	*"The classic model for information security defines three objectives: Confidentiality, Integrity, and Availability. Network and information security, as defined in the ENISA regulation 526/2013, means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the Availability, Authenticity,*

[207] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[208] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[209] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[210] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[211] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[212] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[213] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.
[214] Preservation: the act, process, or result of preserving something: the activity or process of keeping something valued alive, intact, or free from damage or decay (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/preservation), accessed on 25. 8. 2021.
[215] ISO/IEC 27000, Fifth edition, 2018.
[216] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/information_security, accessed on 1. 7. 2021.

	Integrity and Confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems. Information security, network and information security are subsets of cybersecurity.” [217]
NATO 1	*“The protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. INFOSEC (electronic information security). Note: Information in document form will be protected by the use of appropriate document security measures. Information in electronic form will be protected by the use of appropriate INFOSEC measures. The application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves.”* [218]
NATO 2	*“The protection of information against unauthorised disclosure, transfer, modification or destruction, whether accidental or intentional. Source: AComP-01/IEC 721 (adopted by NATO) Comments: AComP-01 790.NN.33 Notes: Information may exist in the human mind, in document form and in electronic form. Information in the human mind will be protected by the use of appropriate personnel security measures. Information in document form will be protected by the use of appropriate document security measures. Information in electronic form will be protected by the use of appropriate INFOSEC measures. “* [219]
CCDCOE	*NONE*
Czech Republic	Provided definition from The Cyber Security Glossary:[220] *“Security (protection) of confidentiality, integrity and availability of information. Implementation of general security measures and procedures for: (1) protection of information against loss or compromise (loss of confidentiality, integrity and reliability), or as the case may be for their detection and adoption of remedial actions. (2) Continuation of information accessibility and ability to work with them within the scope of functional rights. Measures information security cover security of computers, transmission, emissions and encryption security and exposing threats to facts and systems and prevention thereof.”* [221]
Estonia*	*“Estonia prefers to use the term cybersecurity that is defined by the Estonian Cybersecurity Strategy as “a condition where network and information systems are protected by the realisation of threats.”* [222]
Greece	*“The practice of applying security measures for the protection of information from unauthorized access and disclosure or disruption of authorized access.”* [223]

[217] ENISA, ENISA overview of cybersecurity and related terminology, Version 1, September 2017, url: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, accessed on 1. 7. 2021.

[218] NATO, AAP-31, Ed.: 3A, version 1, March 2005.

[219] Ibid.

[220] Jirásek P., Novák L., Požár J., 2013.

[221] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[222] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[223] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

Japan	*"The basic principal of information security is to ensure "confidentiality", "integrity", and "availability" of the information handled by Agencies according to the degree of importance of information, and it is a fundamental responsibility for each government agency to duly implement measures to ensure information security."*[224]
Luxembourg*	*NONE. "In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case)."* [225] *For the purposes of the Grand-Ducal Decree of 9 May 2018 on establishing the governance of information security management, "information security" means security around classified and unclassified information systems installed and operated by the State."*[226]
Portugal	*"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."* [227]
Slovakia	*Uses NATO accepted definition.* [228]
State 1	*"There is not approved definition of Information Security. The NAF considers all procedures and measures to ensure information confidentiality."*[229]
State 2	*"Ability of network and information systems to resist, at a given level of confidence, any action that compromises the ability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems."* [230]
State 3	*"As per the Information Security Act, information security means protection, security and defence of the information environment from unauthorised access, use, disclosure, interference with, modification or destruction, in order to provide confidentiality, authenticity, integrity and availability."* [231]
State 4	*"The overall measures taken to safely and securely use the information and the IT systems and to detect the unauthorized access."* [232]
United Kingdom	*"The secure storage, use, processing or transmission of information."*[233]

[224] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[225] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[226] Ibid.

[227] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[228] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[229] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[230] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[231] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[232] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[233] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.

10.3 Cybersecurity

ISO	N/A
ISO	*“Cybersecurity/Cyberspace security*[234]*. Preservation*[235] *of confidentiality, integrity and availability of information in Cyberspace (NOTE: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved). Cybersafety: condition of being protected*[236] *against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable (NOTE: This can take the form of being protected from the event or from the exposure to something that causes health or economic losses. It can include protection of people or of assets. Safety*[237] *in general is also defined as the state of being certain that adverse effects will not be caused by some agent under defined conditions).”* [238]
NIST 1	*“(1) Prevention*[239] *of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”*[240]
NIST 2	*“The ability to protect or defend the use of cyberspace from cyber attacks.”* [241]

[234] Security: the state of being protected or safe from harm (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/security, accessed on 25. 8. 2021). Safety versus security, As nouns the difference between safety and security is that safety is the condition or feeling of being safe; security; certainty while security is (uncountable) the condition of not being threatened, especially physically, psychologically, emotionally, or financially (Wikidiff, url: https://wikidiff.com/safety/security, accessed on 25. 8. 2021).

[235] Preservation: the act, process, or result of preserving something: the activity or process of keeping something valued alive, intact, or free from damage or decay (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/preservation, accessed on 25. 8. 2021. As nouns the difference between preservation and protection is that preservation is the act of preserving; care to preserve; act of keeping from destruction, decay or any ill while protection is the process of keeping (something or someone) safe (Wikidiff, url: https://wikidiff.com/preservation/protection, accessed on 25. 8. 2021).

[236] Protection: the act of protecting: the state of being protected (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/protection, accessed on 25. 8. 2021). As verbs the difference between preserve and protect is that preserve is to protect; to keep; to maintain the condition of while protect is to keep safe; to defend; to guard; to prevent harm coming to (Wikidiff, url: https://wikidiff.com/preserve/protect, accessed on 25. 8. 2021).

[237] Safety: freedom from harm or danger: the state of being safe (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/safety, accessed on 25. 8. 2021). As adjectives the difference between secure and safe is that secure is free from attack or danger; protected while safe is not in danger; free from harm's reach (Wikidiff, url: https://wikidiff.com/secure/safe, accessed on 25. 8. 2021).

[238] ISO/IEC 27032, First edition, 2012.

[239] Prevention; the act of preventing or hindering (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/prevention, accessed on 25. 8. 2021). As nouns the difference between prevention and protection is that prevention is (obsolete) the act of going, or state of being, before while protection is the process of keeping (something or someone) safe (Wikidiff, url: https://wikidiff.com/prevention/protection, accessed on 25. 8. 2021).

[240] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/cybersecurity, accessed on 1. 7. 2021.

[241] Ibid.

NIST 3	*"The process of protecting information by preventing, detecting, and responding to attacks."* [242]
NIST 4	*"The prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems."* [243]
EU	*"Cybersecurity comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats. Cybersecurity covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security)."* [244]
NATO	*"The application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation."* [245]
CCDCOE	NONE
Czech Republic	Provided definition from The Cyber Security Glossary:[246] *"Collection of legal, organizational, technological and educational means aimed at providing protection of cyberspace."* [247]
Estonia*	*"A state of being where network and information systems are protected from threats. (The term for the process of ensuring this protection is "küberturve" as opposed to "küberturvalisus", the direct translation of "cybersecurity")."* [248]
Greece	Not officially defined yet. [249]
Japan	The Basic Act on Cybersecurity reads, Article 2: *"For the purposes of this Act, the term "Cybersecurity" means the necessary measures that are needed to be taken to safely manage information, such as prevention against the leak, disappearance, or damage of information which is stored, sent, in transmission, or received by electronic, magnetic, or other means unrecognizable by natural perceptive functions (hereinafter in this section referred to as "Electronic or*

[242] Ibid.

[243] Ibid.

[244] ENISA, ENISA overview of cybersecurity and related terminology, Version 1, September 2017, url: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, accessed on 1. 7. 2021.

[245] NATO, AJP-3.20, Edition A, version 1, January 2020.

[246] Jirásek P., Novák L., Požár J., 2013.

[247] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[248] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[249] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

	Magnetic Means"); and to guarantee the safety and reliability of information systems and information and telecommunications networks (including necessary preventive measures against malicious activities toward electronic computers through information network or storage media for information created by electronic or magnetic means (hereinafter referred to as "Electronic or Magnetic Storage Media")), and that those states are appropriately maintained.” [250]
Luxembourg*	NONE. *“In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case).”* [251] *“The application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non- repudiation (NATO Definition according to AJP 3.2, used in the Cyber Defence Strategy).”* [252]
Portugal	*“The application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.”* [253]
Slovakia	*“A state in which the networks and information systems have the capability to resist, at a certain reliability level, against any conduct threatening the availability, authenticity, integrity or confidentiality of the stored, transferred, or processed data or related services provided and available through these networks and information systems. (Legal Act No. 69/2018).”* [254]
State 1	*“According the Cybersecurity Strategy 2019-2022, cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Nevertheless this definition is not used in legal acts, as it is stated in the report “Going Digital” published by Organisation for Economic Co-operation and Development in 2021.”* [255]
State 2	*“Information systems’ resistance to acts disrupting the confidentiality, integrity, availability and authenticity of data transmitted therein or related to services those systems offer.”* [256]

[250] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[251] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[252] Ibid.
[253] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[254] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[255] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[256] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

State 3	*“As per the Information Security Act, cybersecurity denotes the ability to safeguard, protect and defend cyberspace from cyber threats, incidents and cyber-attacks.”*[257]
State 4	*“The technology, processes and the required actions to protect the networks, hardware/software and the entities of the IT systems from the cyberattacks and unauthorized access.”*[258]
United Kingdom	*“The protection of devices, services and networks – and the information on them – from theft or damage.”*[259]

10.4 Cyber defence

UN	NONE
ISO	NONE
NIST	*“Actions normally created within DoD cyberspace for securing, operating, and defending the DoD information networks. Specific actions include protect, detect, characterize, counter, and mitigate.”* [260]
EU	*“Cyber defense refers to a variety of defensive mechanisms that could be used to mitigate or respond to cyber attacks.”* [261]
NATO 1	*“The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.”* [262]
NATO 2	*“Cyber defence activities are a pivotal element of CIS security - enabling delivery and management of CIS services in response to malicious actions perpetuated through cyberspace. Cyber defence is defined as the means to achieve and execute defensive measures to counter cyber attacks and mitigate their effects, and thus preserve and restore the security of communication, information, and other electronic systems.”* [263]

[257] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[258] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[259] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.

[260] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/cyberspace_defense, accessed on 1. 7. 2021. NIST define four type of cyber defence: (1) Active cyber defence: Synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. (2) Proactive cyber defense: A continuous process to manage and harden devices and networks according to known best practices. (3) Integrated Adaptive Cyber Defense: no definition. (4) Regenerative cyber defense: The process for restoring capabilities after a successful, large scale cyberspace attack, ideally in a way that prevents future attacks of the same nature. (Ibid)

[261] ENISA, ENISA overview of cybersecurity and related terminology, Version 1, September 2017, url: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, accessed on 1. 7. 2021.

[262] NATO, AAP-06, Edition 2020.

[263] NATO, AJP-6, Edition A, version 1, February 2017.

CCDCOE	*"Active Cyber Defence: The taking of proactive defensive measures outside the defended cyber infrastructure. A 'hack-back' is a type of active cyber defence."* [264]
Czech Republic	*"The Czech Government´s* ***understands*** *cyber defence as an autonomous and specific branch of a wider cybersecurity concept. In this context, cyber defence is perceived as part of state defence ensured on the basis of the Act on Ensuring Defence of the Czech Republic. Cyber defence differs from cybersecurity mainly in the nature and intensity of attacks, with no possibility to define exact criteria."* [265]
Estonia*	*"Cyber Defence – implementation of measures to prevent and deter cyber attacks; the term is used in the context of State defence. (The definition is based on the Estonian Cybersecurity Strategy 2019-2022).* [266]
Greece	Not officially defined yet. [267]
Japan	*"The term "Cyber defense" is not defined by national law and its universally accepted definition does not exist."* [268]
Luxembourg*	NONE. *"In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case)."* [269] *"The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems (NATO Definition according to AAP-06 (2019), used in the Cyber Defence Strategy)."* [270]
Portugal	*"Prepare for, prevent, detect, respond to, recover from and learn lessons from attacks, damage or unauthorized access affecting information infrastructures (including military and civil networks) that support and enable the conduct of NATO/National military tasks and Crisis Management Operations."* [271]
Slovakia	*"Defence of the State in the cyber domain trough measures focused on handling of serious cyber security incident in accordance with a specific legal act, and defending of the Objects of Extraordinary Importance, other Importance Objects, and Critical Infrastructure Elements from cyber-attacks."* [272]
State 1	*There is not approved definition of Cyber defence. "The NAF considers Cyber Defence as the procedures and measures to protect national ICT."* [273]

[264] Tallinn manual 2.0 on the international law applicable to cyber operations, 2017, p. 563.
[265] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[266] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[267] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[268] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[269] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[270] Ibid.
[271] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[272] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[273] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

State 2	*"The means to achieve and executive defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communications, information or other electronic systems, or the information that is stored, processed or transmitted on these systems."*[274]
State 3	*"As per the Information Security Act, cyber defence denotes a set of measures and operations taken by the state to discourage, disable, prevent or repel cyber-attacks in information environments."*[275]
State 4	*"The defence activities to ensure the durability of the entities in cyberspace, which encompasses the active defence and proactive measures."*[276]
United Kingdom	*"The protection of devices, services and networks – and the information on them – from theft or damage."*[277]

10.5 Cyber resilience

UN	NONE
ISO	NONE
NIST	*"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."* [278]
EU 1	*"Cyber resilience refers to the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack."* [279]
EU 2	*"Resilience means the ability to prevent, resist, mitigate, absorb, accommodate to and recover from an incident that disrupts or has the potential to disrupt the operations of a critical entity."* [280]
NATO	*"The overall technical and procedural ability of systems, organizations and operations to withstand cyber incidents and, where harm is caused, recover from them with no or acceptable impact on mission assurance or continuity."* [281]
CCDCOE	NONE

[274] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[275] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[276] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[277] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.

[278] NIST, Computer Security Resource Center, Glossary, url: https://csrc.nist.gov/glossary/term/cyber_resiliency, accessed on 1. 7. 2021.

[279] ECB, What is cyber resilience?, url: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html, accessed on 25. 8. 2021.

[280] EU, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities, COM(2020) 829 final, 2020/0365(COD).

[281] NATO, AAP-06, Edition 2020.

Czech Republic	Provided definition from The Cyber Security Glossary:[282] *“Capability of an organization, system or network to resist threats and defend itself against the influence of outages.”* [283]
Estonia*	*“Cyber resilience – Condition, situation, or attribute where an organization would be capable of providing their services despite of and during cyber attacks.”*[284]
Greece	Not officially defined yet. [285]
Japan	*“The term “Cyber resilience” is not defined by national law and its universally accepted definition does not exist.”* [286]
Luxembourg*	NONE. *“In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case).”* [287]
Portugal	*“Ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from deliberate cyber-attacks, accidents or naturally occurring threats or incidents.”*[288]
Slovakia	Uses NATO and EU generally accepted definition. [289]
State 1	*“According the Cybersecurity Strategy 2019-2022, Information and Communication Technologies (ICT) resilience is the ability of ICT to withstand, recover and change in the event of external disruption, such as a cyber-attack or a natural disaster.* [290]
State 2	*“The overall technical and procedural ability of systems, organisations and operations to withstand cyber incidents and, where harm is caused, to recover from it with no or acceptable impact on mission assurance or continuity.”*[291]
State 3	*“The concept of Cyber resilience is not per se legally defined, but it is inherently related to the ultimate goal of cybersecurity and cyber defence, namely the ability to preserve or re-establish the security of cyberspace on the level that is required for the smooth functioning of the state.”*[292]
State 4	*“The ability to identify the entities that need to be protected, take precautions against cyberattacks, detect the attacks in timely manner and respond the incidents and maintain business continuity according to a plan.”*[293]

[282] Jirásek P., Novák L., Požár J., 2013.
[283] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[284] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[285] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[286] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[287] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[288] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[289] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[290] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[291] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[292] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[293] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

United Kingdom	*"The ability of an organisation or platform to withstand and/or recover from malicious events in cyberspace."*[294]

10.6 Information environment

UN	NONE
ISO	NONE
NIST	*"The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."* [295]
EU	NONE
NATO 1	*"An environment comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs."* [296]
NATO 2	*"The Information environment comprises the information itself, the individuals, organisations and systems that receive, process and convey the information, as well as the cognitive, virtual and physical space in which this occurs."* [297]
CCDCOE	NONE
Czech Republic	NONE [298]
Estonia*	NONE [299]
Greece	Not officially defined yet. [300]
Japan	The term "Information environment" is not defined by national law and its universally accepted definition does not exist.[301]
Luxembourg*	NONE. *"In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case)."* [302]
Portugal	*"Aggregate of individuals, organizations, and/or systems that collect, process, or disseminate information, also included is the information itself."* [303]

[294] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.
[295] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/information_environment, accessed on 1. 7. 2021.
[296] NATO, NATO Glossary of terms and definitions, AAP-06, Edition 2020.
[297] NATO, Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, Edition A, version 1, January 2020.
[298] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[299] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[300] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[301] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[302] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[303] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

Slovakia	Uses NATO and EU generally accepted definition. [304]
State 1	*"There is not approved definition of Information environment. The information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision making."*[305]
State 2	*"Numerous social, cultural, cognitive, technical and physical attributes that act upon and impact knowledge, understanding, beliefs, world views and ultimately, actions of on individual, group, system, community or organisation. Include systems and their use of data."* [306]
State 3	*"As per the Information Security Act, the information environment means a cluster of social networks and cyberspace, including information."*[307]
State 4	*"Any environment that stores, processes and transmits data. "* [308]
United Kingdom	*"An environment comprised of the information itself; the individuals, organisations and systems that receive, process and convey the information; and the cognitive, virtual and physical space in which this occurs."*[309]

10.7 Cyberspace

UN	NONE
ISO	*"Cyberspace: complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."* [310]
NIST 1	*"A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*[311]
NIST 2	*"The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."*[312]
NIST 3	*"The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."* [313]

[304] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[305] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[306] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[307] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[308] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[309] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.
[310] ISO/IEC 27032, First edition, 2012.
[311] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/cyberspace, accessed on 1. 7. 2021.
[312] Ibid.
[313] Ibid.

EU	*"Cyber space is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information."* [314]
NATO	*"The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data."* [315]
CCDCOE	*"The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks."* [316]
Czech Republic	Provided definition from The Cyber Security Glossary:[317] *"Digital environment enabling the origin, processing and exchange of information, made up of information systems and the services and networks of electronic communications."* [318] Definition from the Cyber Security Act: *"Digital environment enabling the creation, processing and exchange of information created by information systems and services and electronic communication networks."*[319]
Estonia*	*"An environment created by the connection of network and information systems."* [320]
Greece	Not officially defined yet. [321]
Japan	*"The term "Cyberspace" is not defined by national law and its universally accepted definition does not exist."* [322]
Luxembourg*	NONE. *"In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case)."* [323]
Portugal	*"Global domain made from the network of information technology infrastructures (including the Internet), telecommunications networks, information systems, processors and integrated control mechanisms (based on US JP 3-12). Cyber space includes transported digital information as well as operators' network infrastructures of online services."*[324]

[314] ENISA, ENISA overview of cybersecurity and related terminology, Version 1, September 2017, url: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, accessed on 1. 7. 2021.

[315] NATO, AJP-3.20, Edition A, version 1, January 2020.

[316] Tallinn manual 2.0 on the international law applicable to cyber operations, 2017, 564.

[317] Jirásek P., Novák L., Požár J., 2013.

[318] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[319] Ibid.

[320] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[321] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[322] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[323] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[324] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

Slovakia	*"A global dynamic open system of networks and information systems consisting of activated elements of the cyberspace, natural persons performing its activities at an acceptable level determined in advance."* (Legal Act No. 69/2018).[325]
State 1	*There is not approved definition of Cyberspace. "The NAF considers Cyberspace as a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.* [326]
State 2	*"Time-dependent set of tangible and intangible assets, which store and/or transfer electronic information."* [327]
State 3	*"As per the Information Security Act, Cyberspace is a global information environment created by means of electronic communications networks and information systems. Cyberspace facilitates the creation, processing and exchange of information."* [328]
State 4	*"The physical digital infrastructure, communication networks and electromagnetic spectrum built on top of these infrastructures, the operating systems, applications, functional services running on these networks, the data that produced, stored, transmitted, the identity, behaviour and thoughts on the conceptual level, including human interaction in all levels, a physical, virtual and intellectual space which is also geographically independent."* [329]
United Kingdom	*"An operating environment consisting of the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the psychical, virtual and cognitive domains."*[330]

10.8 Cyber attack

UN	NONE
ISO	ISO does not use "cyber attack" but solely an *"attack: attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset."* [331] *"Cybercrime: criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime."* [332]
NIST	*"Cyber attack. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously*

[325] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[326] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[327] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[328] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[329] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[330] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.

[331] ISO/IEC 27000, Fifth edition, 2018; ISO/IEC 27032, First edition, 2012.

[332] ISO/IEC 27032, First edition, 2012.

	controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.” [333]
EU	*“Cyber attacks cover all cyber incident triggered by malicious intent where damages, disruptions or dysfunctionalities are caused. Cybercrime refers to any crime/criminal activity facilitated by or using cyber space. Cyber sabotage refers to any sabotage activity facilitated by or using cyber space. Cyber espionage: we understand 2 types of espionage vectors: (a) state espionage (intelligence, when state actors are involved) or (b) industrial espionage (when commercial actors are involved). Cyberwarfare refers to any action by a state, group or criminal organisation facilitated by or using cyber space targeting another state. “* [334]
NATO	NONE. Currently under discussion at the Allied Joint Operations Doctrine Working Group.
CCDCOE	*“A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. The term ‘cyber espionage’ refers to any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information. Cyber espionage involves, but is not limited to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information. “*[335]
Czech Republic	Definition from The Cyber Security Glossary:[336] *“Attack on IT infrastructure having the objective of causing damage and obtaining sensitive or strategically important information. It is used most often in the context of either politically or militarily motivated attacks.”* [337]
Estonia*	“An intentional act, committed through the use of network and information systems, with the intention of causing harm or damage.” [338]
Greece	Not officially defined yet. [339]
Japan	*“The term “Cyber attack” is not defined by national law and its universally accepted definition does not exist. “In case of MOD/SDF the term is defined as electronic attacks against information systems via networks (the Information Assurance Directive 2(5)).”* [340]

[333] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/Cyber_Attack, accessed on 1. 7. 2021.

[334] ENISA, ENISA overview of cybersecurity and related terminology, Version 1, September 2017, url: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, accessed on 1. 7. 2021.

[335] Tallinn manual 2.0 on the international law applicable to cyber operations, 2017, p. 564.

[336] Jirásek P., Novák L., Požár J., 2013.

[337] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[338] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[339] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[340] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

Luxembourg*	NONE. *"In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case)."* [341]
Portugal	*"An act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems."*[342]
Slovakia	NONE. Uses of the term Cyber Security Incident. [343]
State 1	There is not approved definition of Cyber attack. *"The NAF considers Cyber-attack as an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."* [344]
State 2	*"An act or action initiated in cyberspace to disrupt, deny, degrade or destroy by compromising communication, information and other electronic systems, or the information that is stored, processed or transmitted on these systems."* [345]
State 3	*"As per the Information Security Act, Cyber-attack means an attack through cyberspace for the purpose of maliciously destroying, exposing, controlling or changing, disabling, collecting or obstructing any part of cyberspace, including with regard to information essential for the smooth functioning of the state."* [346]
State 4	*"The activities to partially or completely, disrupt, destroy, change, exploit the entities of cyberspace via cyber tools."* [347]
United Kingdom	*"Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means."*[348]

10.9 Cyber incident

UN	NONE
ISO	*"Event[349]: occurrence or change of a particular set of circumstances (NOTE: 1. An event can be one or more occurrences, and can have several causes. 2. An*

[341] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[342] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[343] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[344] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[345] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[346] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[347] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[348] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.

[349] Event: something that happens; occurrence (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/event, accessed on 25. 8. 2021).
Cyber security event: is a change in the normal behavior of a given system, process, environment or workflow (Examples: An employee flags a suspicious email; A security lapse occurs due to a server outage; Downloaded software (authorized or unauthorized) to a company device) (BitLyth, What Is a Cybersecurity Event?, url: https://www.bitlyft.com/resources/cybersecurity-event-vs-incident-whats-the-difference, accessed on 25. 8. 2021).

	event can consist of something not happening. 3. An event can sometimes be referred to as an “incident” or “accident”).” “Information security event: identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.” “Information security incident[350]*: single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.”* [351]
NIST	*“Cyber incident: Actions*[352] *taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.”*[353] *(1) “Intrusion (Synonym: Penetration). A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.”* [354] *(2) “Event. (a) Any observable occurrence in an information system. (b) Any observable occurrence in a network or system. (c) Something that occurs within a system or network. (d) Any observable occurrence in a network or information system. (e) Any observable occurrence on a manufacturing system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, capabilities, or reputation). (f) Occurrence or change of a particular set of circumstances.”* [355] *(3) “Security-relevant event. Any event that attempts to change the security state of the system (e.g., change access controls, change the security level of a user, change a user password). Also, any event that attempts to violate the security policy of the system (e.g., too many logon attempts).”* [356]
EU	*“Cyber incident. Any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, independent if it’s natural or human made; malicious or non-malicious intent; deliberate, accidental*

Event: is an observed (identifiable occurrence) to the normal behaviour of a system, environment, process, workflow or person, which could be theoretically relevant to information security. (Simplicable, Security Events vs Security Incident, url: https://simplicable.com/new/security-event-vs-security-incident, accessed on 25. 8. 2021. Daniel Miessler, The Difference Between Events, Alerts, and Incidents, url: https://danielmiessler.com/study/event-alert-incident, accessed on 25. 8. 2021)

[350] Incident: an occurrence of an action or situation that is a separate unit of experience; happening (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/incident, accessed on 25. 8. 2021). Incident: is a change in a system that negatively impacts the organization, municipality, or business. For example, an incident might take place when a cyber attack occurs (Examples: replying to a phising mail, a brute force attack compromise a password, equipment with sensitive data is stolen).

Incidents refer to the more specific events that cause harm to your environment. (BitLyth, What Is an Incident?, url: https://www.bitlyft.com/resources/cybersecurity-event-vs-incident-whats-the-difference, accessed on 25. 8. 2021). Incident: is an event that affects the confidentiality, integrity, and/or availability (CIA triad) at an organization in a way that damage or risk its information security. (Simplicable, Security Events vs Security Incident, url: https://simplicable.com/new/security-event-vs-security-incident, accessed on 25. 8. 2021; Daniel Miessler, The Difference Between Events, Alerts, and Incidents, url: https://danielmiessler.com/study/event-alert-incident, accessed on 25. 8. 2021)

[351] ISO/IEC 27000, Fifth edition, 2018.

[352] Action: a thing done, deed; Actions: behavior, conduct. (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/action, accessed on 25. 8. 2021).

[353] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/cyber_incident, accessed on 1. 7. 2021.

[354] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/intrusion, accessed on 1. 7. 2021.

[355] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/event, accessed on 1. 7. 2021.

[356] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/security_relevant_event, accessed on 1. 7. 2021.

	or due to incompetence; due to development or due to operational interactions is called cyber incident. Also we call cyber incident any incident generated by any of cyber space components even if the damage/disruption, dysfunctionality is caused outside the cyber space." "Cyber accident. To support a 'grading' of cyber incidents, we define cyber accidents as any occurrence associated with cyber space causing significant damage to cyber space or any other asset (has performance impact, requires repairs, replacement) or causing personal injury." [357]
NATO	*"Any detected anomaly compromising or that has the potential to compromise communication, information or other electronic systems or the information that is stored, processed or transmitted in these systems."* [358]
CCDCOE	NONE
Czech Republic	*The Cyber Security Act defines cyber incident as:* *"a breach in the security of information in information systems, a breach in the security of service provision or a breach of security and integrity of electronic communication networks due to the cybersecurity event."* [359]
Estonia*	*"Any event in the network and information system compromising or having an adverse effect on the security of the system."* [360]
Greece	Not officially defined yet. [361]
Japan	*"The term "Cyber incident" is not defined by national law and its universally accepted definition does not exist."* [362]
Luxembourg*	*According to GOVCERT:* *"An information security event is an identified occurrence in a system, service or network state that indicates a possible breach of information security policy, a failure of safeguards, or a previously unknown situation that may be security relevant."* [363] *An information security incident (or computer incident) is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations or threatening information security, where "information security" means preservation of confidentiality, integrity and availability of information.* [364]

[357] ENISA, ENISA overview of cybersecurity and related terminology, Version 1, September 2017, url: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, accessed on 1. 7. 2021.

[358] NATO, Approval of Terminology Proposals, AC/322-N(2019)0043-REV 1-AS1 (INV).

[359] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[360] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[361] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[362] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[363] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[364] Ibid.

Portugal	*“An unauthorized or unexpected CIS event where automated measures have failed, **whose impact is not severe**, and recovery can be achieved through the involvement of cyber experts.”*[365]
Slovakia	*“Any occurrence that as a consequence of disruption of the networks and information system security, or violation of the security policy or binding methodology, has a negative impact on cybersecurity or which results in:* *1. The loss of data confidentiality, destruction of data or disruption of system integrity,* *2. Limitation or rejection of availability of essential services or digital service,* *3. High probability of compromising the activities of essential services or digital service, or* *4. Threat to information security. (Legal Act No. 69/2018).”* [366]
State 1	*“According Law on the Security of Information Technologies, an information technologies security incident is a harmful event or offence as a result of which the integrity, availability, or confidentiality of information technologies is endangered.”*[367]
State 2	*“Any detected anomaly compromising or that has the potential to compromise communication, information or other electronic systems or the information that is stored, processed or transmitted in these systems.”*[368]
State 3	*“The concept of Cyber incident is not per se legally defined. However, the Information Security Act does define the concept of an incident which, namely, denotes any event having an actual adverse effect on the security of network and information systems.”*[369]
State 4	*“Any unexpected incident on cyberspace ranging from unauthorized access to deliberate malicious activities.”*[370]
United Kingdom	*“A breach of the security rules for a system or service – most commonly;* *1. Attempts to gain unauthorised access to a system and/or to data.* *2. Unauthorised use of systems for the processing or storing of data.* *3. Changes to a systems firmware, software or hardware without the system owner’s consent.* *4. Malicious disruption and/or denial of service.”*[371]

[365] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[366] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[367] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[368] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[369] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[370] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[371] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.

10.10 Cyber operation

UN	NONE
ISO	N/A
NIST	"The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." [372]
EU	NONE
NATO 1	*"Actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders' objectives."* [373]
NATO 2	*"Actions in or through cyberspace intended to preserve own and friendly freedom of action in cyberspace and/or to create effects to achieve military objectives. Consist of four areas (CIS Infrastructure Operations; Defensive Cyberspace Operations; Cyberspace Intelligence, Surveillance and Reconnaissance; Offensive Cyberspace Operations)."* [374]
CCDCOE	*"The employment of cyber capabilities to achieve objectives in or through cyberspace. In this Manual, the term is generally used in an operational context (see also 'cyber activity')." "Cyber Activity: Any activity that involves the use of cyber infrastructure or employs cyber means to affect the operation of such infrastructure. Such activities include, but are not limited to, cyber operations."* [375]
Czech Republic	Czech has decided to withhold this information.[376]
Estonia*	*"Cyber Operation – activity that is taking place in the network and information systems environment for a specific goal with effects on cyber security; the definition is used in the context of State's security. (The definition is based on the Estonian Cybersecurity Strategy 2019-2022)."* [377]
Greece	Not officially defined yet. [378]
Japan	*"The term "Cyber operations" is not defined by national law and its universally accepted definition does not exist."* [379]

[372] NIST, Glossary, url: https://csrc.nist.gov/glossary/term/cyberspace_operations, accessed on 1. 7. 2021.
[373] NATO, AJP-3.20, Edition A, version 1, January 2020.
[374] NATO, High Level Taxonomy of Cyberspace Operations, IMSM-0222-2018.
[375] Tallinn manual 2.0 on the international law applicable to cyber operations, 2017, p. 564.
[376] Czech Republic, National Cyber and Information Security Agency (NÚKIB), Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[377] Government of Estonia (the Ministry of Economic Affairs and Communication, the State Information Systems Authority, the Ministry of Defence), Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[378] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[379] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

Luxembourg*	NONE. *"In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case)."* [380]
Portugal	*"Actions to achieve (military) goals using cyber capabilities."* [381]
Slovakia	Uses NATO accepted definition (AJP 3.20). [382]
State 1	*"There is not approved definition of Cyber Operation. The NAF considers Cyber Operation as the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."* [383]
State 2	*"Actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve the commander's objectives."* [384]
State 3	NONE [385]
State 4	*"The activities to gain tactical advantage in cyberspace, such as:* *CIS Operations,* *Defensive Cyber Operations,* *Offensive Cyber Operations,* *Cyber Intelligence, Surveillance and Reconnaissance."* [386]
United Kingdom	*"The planning and synchronisation of activities in and through cyberspace to enable freedom of manoeuvre and to achieve military objectives."*[387]

10.11 Aggression

UN	*"Article 1: Aggression*[388] *is the use of armed force by a State (or group of States) against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition. Article 2: The First use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed*

[380] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[381] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[382] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[383] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[384] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[385] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[386] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

[387] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.

[388] Aggression: 1: a forceful action or procedure (such as an unprovoked attack) especially when intended to dominate or master; 2: the practice of making attacks or encroachments especially: unprovoked violation by one country of the territorial integrity of another warned that any act of aggression could start a war; 3: hostile, injurious, or destructive behaviour or outlook especially when caused by frustration. (Merriam-Webster, Dictionary, url: https://www.merriam-webster.com/dictionary/aggression, accessed on 25. 8. 2021)

	would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity. Article 3: Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of article 2, qualify as an act of aggression: (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof, (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State; (c) The blockade of the ports or coasts of a State by the armed forces of another State; (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State; (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement; (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State; (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein. Article 4: The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter. Article 5: a. No consideration of whatever nature, whether political, economic, military or otherwise, may serve as a justification for aggression. b. A war of aggression is a crime against international peace. Aggression gives rise to international responsibility. c. No territorial acquisition or special advantage resulting from aggression is or shall be recognized as lawful. Article 6: Nothing in this Definition shall be construed as in any way enlarging or diminishing the scope of the Charter, including its provisions concerning cases in which the use of force is lawful." [389]
ISO	N/A
NIST	NONE
EU	NONE
NATO	NONE
CCDCOE	*"Aggression is one of the situations (General Assembly Resolution 3314 (XXIX)), and in which the UN Security Council may employ its powers under Chapter VII of the UN Charter."* [390]
Czech Republic	Definition provided by the Ministry of Interior: *"Use of the armed forces of a State against the sovereignty, territorial inviolability or political independence of the other State or for any other purpose incompatible with the Charter of the United Nations."* [391]

[389] UN, Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), April 1974.

[390] Tallinn manual 2.0 on the international law applicable to cyber operations, 2017, 339.

[391] Czech Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.

Estonia*	*"An act of Aggression – action(s) in or through cyberspace that project power to create effects that help to achieve military objectives."*[392]
Greece	Not officially defined yet.[393]
Japan	*"The term "Aggression" is not defined by national law and its universally accepted definition does not exist."*[394]
Luxembourg*	NONE. *"In general, Luxembourg does not create or use its own definitions and prefers to use a widely accepted one, i.e. EU or NATO (which should be the same and is not currently the case)."*[395]
Portugal	*"Means the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."*[396]
Slovakia	Uses generally accepted understanding.[397]
State 1	*"There is not approved definition of Aggression. Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. The NAF considers cyber aggression as intentional harm delivered by the use of electronic means to a person or a group of people irrespective of their age, who perceive(s) such acts as offensive, derogatory, harmful, or unwanted."*[398]
State 2	NONE[399]
State 3	NONE[400]
State 4	*"Any offensive operation of the hostile that is targeting our networks."*[401]
United Kingdom	*"The use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."*[402]

[392] Estonia, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[393] Greece, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[394] Japan, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[395] Luxembourg, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[396] Portugal, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[397] Slovak Republic, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[398] State 1, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[399] State 2, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[400] State 3, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[401] State 4, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, June 2021.
[402] United Kingdom, Initiatives to improve Cyber Defence capabilities: Questionnaire Part A, July 2021.

11. Appendix 3: Organization charts

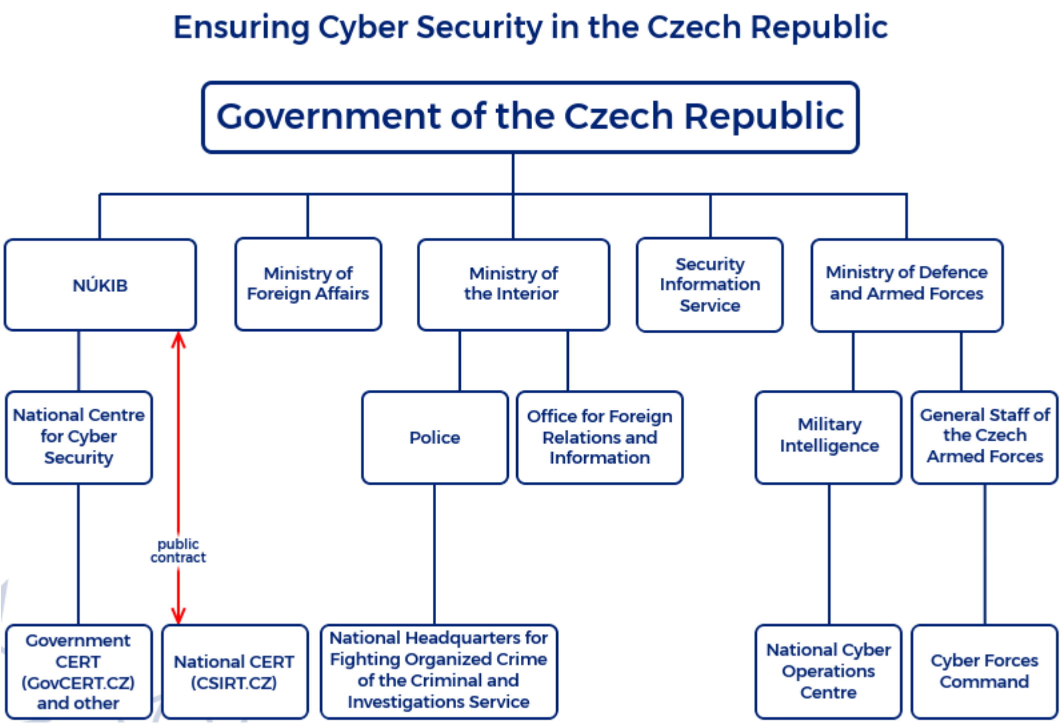

Ensuring Cyber Security in the Czech Republic
Government of the Czech Republic
NÚKIB
Ministry of Foreign Affairs
Ministry of the Interior
Security Information Service
Ministry of Defence and Armed Forces
National Centre for Cyber Security
Police
Office for Foreign Relations and Information
Military Intelligence
General Staff of the Czech Armed Forces
public contract
Government CERT (GovCERT.CZ) and other
National CERT (CSIRT.CZ)
National Headquarters for Fighting Organized Crime of the Criminal and Investigations Service
National Cyber Operations Centre
Cyber Forces Command

Chart 49: Cybersecurity Organizational structure of Czech Republic

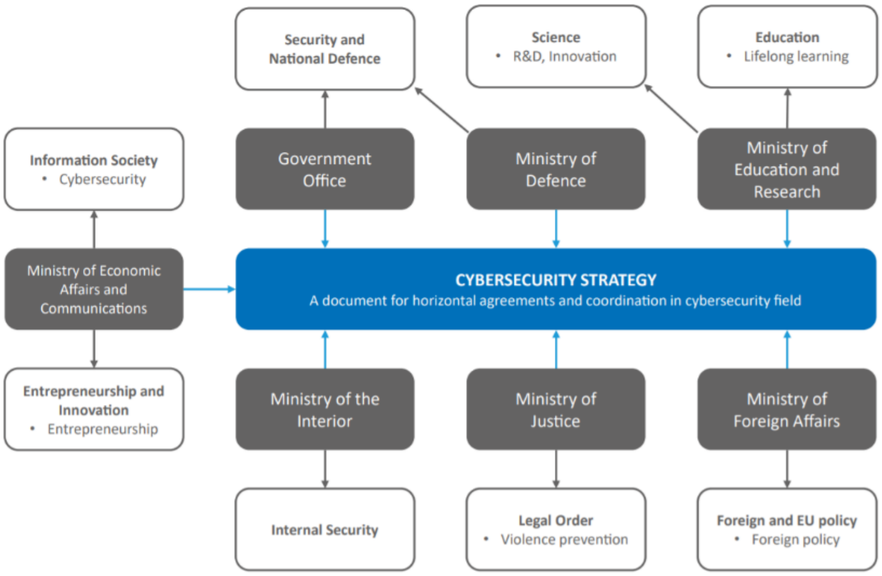


Chart 50: Cybersecurity Organizational structure of Estonia

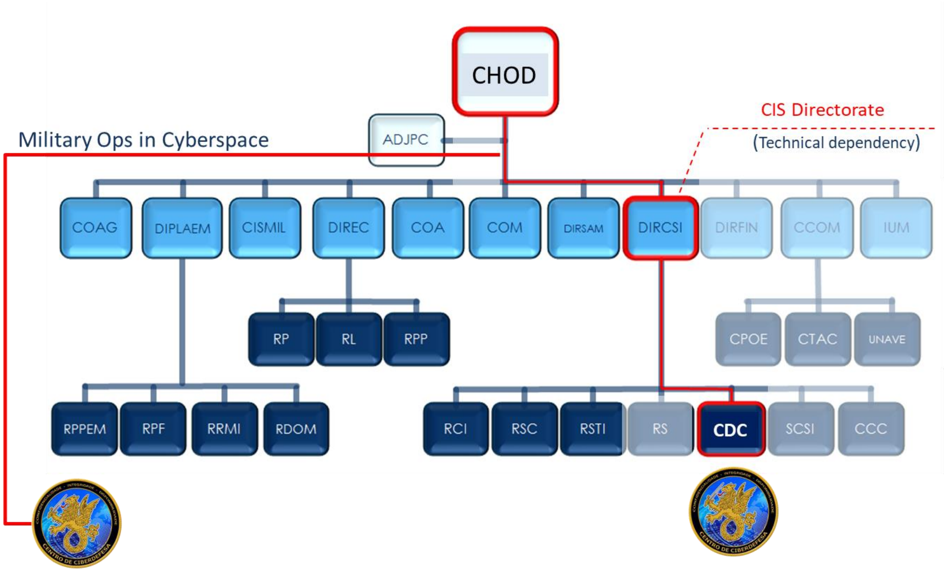


Chart 51: Cyber Defence Organizational structure of Portugal