Cyber as a Domain

Concept and Capabilities

The Hague Centre for Strategic Studies

February 2017

Pieter Bindt, Advisor
Louk Faesen
Nicholas Farnham
Erik Frinking
Alexander Klimburg
Hannes Rõõs
Michel Rademaker, Project Leader

Executive Summary

During the North Atlantic Council in Warsaw 8-9 July 2016, NATO declared that its essential mission is unchanged.[1] It was also stated that NATO has the full range of capabilities necessary to deter and defend against potential adversaries and the full spectrum of threats that could confront the Alliance from any direction.

Cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. For that reason, the Member States agreed in Warsaw that cyber defense is part of NATO's core task of collective defense and NATO's defensive mandate, and that cyberspace is recognized as a separate domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. Furthermore, it will ensure more effective organization of NATO's cyber defense and better management of resources, skills, and capabilities.[2]

The research in this report focused on both the concept of Cyber as a Domain for NATO and on the question whether the existing NATO Strategic Command's cyberspace capabilities cover the whole spectrum of possible cyberspace capabilities that might be required for NATO Strategic Commands to fulfil its ambitions in this new domain. To answer this question, we applied an analytical input-effect framework. Initial analyses showed that the current NATO framework does not fully cover Cyber as a Domain and that gaps exist.

The research concluded that:

1. Current cyber capability requirements and approaches do no take the full scope and depth of Cyber as a Domain in consideration. Future focus by NATO Strategic Commands could be considerably broadened. The scope and depth of NATO's current cyber capability framework should reflect this broader scope.
2. Possible broadening of the current cyberspace analytical framework can be found in emphasizing its deterrence capabilities and strengthening the notion that as a result of considering Cyber as a Domain it contains operational capabilities in their own right.
3. The alignment of thinking and clarity of roles and responsibilities between the NATO Strategic Commands and the Member States, and between the different domains need further attention.
4. There are options to further strengthen NATO cyber capabilities by involving more Non-state actors.
5. The proposed extended framework could create more awareness, thus deepening and operationalizing capability development.

[1] Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016.
[2] Ibid

Colophon

The Hague Centre for Strategic Studies
Lange Voorhout 16 2514 EE
The Hague, The Netherlands
info@hcss.nl

HCSS.NLSponsor and Project Officer

The NCIA The Hague office sponsored this project. The guidance the HCSS project team received was organized via the NCIA project officer Ms. Tamsin Moye with support of LtCol Robert Jensen and project manager Ms. Manisha Parmar.

About the authors

Erik Frinking is the Director of the Strategic Futures Program at HCSS. He holds a Master's degree in Political Science from Leiden University. For almost twenty years, he has been involved in addressing high-level, complex policy issues for a wide variety of European countries and international organizations. Mr. Frinking worked for more than 13 years at the Leiden branch of the RAND Corporation, where he was director of the Education, Science & Technology, and Innovation program.

Louk Faesen is a Cyber Policy expert at HCSS. He holds a Master's degree in Law and Politics of International Security (LLM) from the VU University of Amsterdam. Louk worked previously as a Policy Officer at the Task Force International Cyber Policy of the Ministry of Foreign Affairs of the Netherlands, where he assisted in the substantive preparations of the Global Conference on CyberSpace 2015 (GCCS) and the Global Forum on Cyber Expertise (GFCE) in The Hague and subsequent projects related to the international peace and security of cyberspace, such as the application of international law, confidence building measures (CBMs), and norms of responsible State behavior.

Alexander Klimburg is Director Cyber Policy and Resilience Program at HCSS, an associate (and former research fellow) of Harvard Kennedy School's Belfer Center as well as nonresident senior fellow of the Atlantic Council. He has worked on numerous topics within the wider field of international cybersecurity since 2007, and has acted as an adviser to a number of governments and international organizations on national cybersecurity strategies, international norms of behavior in cyberspace and cyber-conflict (including war, cyber-crime, and cyber-espionage), critical infrastructure protection, and Internet governance. He has participated in international and intergovernmental discussions within the European Union and the Organization for Security and Co-operation in Europe and has been a member of various national, international, NATO, and EU policy and working groups. He is the author of over a dozen articles and publications and has given more then seventy invited talks on the subject. Previously, Klimburg worked for eight years in Vienna as senior adviser at the Austrian Institute of International Affairs and has been closely involved in a

number of European cybersecurity policy initiatives. Prior to this, Klimburg worked on ICT strategy issues in corporate finance and strategy consulting in Europe and Asia.

Hannes Rõõs is a data scientist at HCSS. He has a Master's degree in Sociology from the University of Tartu and also holds Bachelor's degrees in both Political Science and Sociology from the same university. In addition, he studied at the University of Oslo and the University of Mannheim for a total of three semesters. Prior to HCSS, Hannes worked as a research and teaching assistant at the University of Tartu and the associated Centre of Excellence for Strategic Sustainability. At HCSS, Hannes is primarily involved in quantitative data analysis, contributing to all related activities – data gathering, tidying, storing, transformation, modelling, visualization, and communicating the results of the analyses. Mr. Rõõs also assists in the building of interactive web solutions. His substantive research questions include assessing the risks of conflict and instability using a data-driven approach.

Nicholas Farnham is an assistant analyst at HCSS. He has a Bachelor's degree in History and Politics from University College Utrecht. Prior to HCSS, Nicholas has worked at the Institute for Security of Global Affairs at Leiden University. At HCSS, Nicholas is involved with project research assistance, quantitative data analysis, project management support, graphic and concept design, and the drafting and revision of textual documents and reports in addition to various administrative duties.

Michel Rademaker is the project leader and deputy director of HCSS. He gained fifteen years of hands-on experience as an officer of The Netherlands Royal Army, where he held various military operational and staff posts and served a term in former Yugoslavia. After leaving the armed forces, Mr. Rademaker went on to work at TNO The Netherlands as a project and programme manager and senior policy advisor for ten years. As NATO STO project leader, he developed with his teams new serious gaming assessment methods for defence. He conducted several assessments of security technologies, including disruptive ones, and worked on numerous strategic security topics amongst them on cyber security. He has written several book chapters, numerous research reports and articles.

Advisor to the authors

Pieter Bindt is strategic advisor at HCSS, former Director NL Defense Intelligence and Security Service. He has an extensive background in intelligence, security, cyber, Joint/combined military operations and international affairs. In April 2016 he retired as Rear Admiral as Director of the Netherlands Defense Intelligence and Security Service. In this function he served customers at the cabinet, operational, and tactical level. Previously he held several seagoing commands, both on surface ships as on submarines, including command of the integrated, operational, deployable staff of the Royal Netherlands Navy; "Netherlands Maritime Force (NLMARFOR)". Amongst his shore staff functions were Deputy Director Operational Policy and Naval planner at the Joint staff of the Chief of Defense, and analyst at the Submarine Tactics and Weapons Group, Flag Officer Submarines, UK Royal Navy.

Table of Contents

Table of Figures

Table of Tables

1 General Introduction

This study is aimed at exploring and developing the concept of Cyber as a Domain for the NATO Communications and Information Agency (NCIA) at the request of NATO Allied Command Transformation (ACT).

HCSS was asked to address the concept of cyber as a domain and analyze and develop the scoping of the concept by addressing the question whether the existing NATO cyber capabilities covered the whole spectrum of possible cyber capabilities that might by required for NATO Strategic Commands to fulfil its ambitions declaring cyber its fourth domain of operations. For that latter part, an analytical framework was applied.

To answer these questions HCSS used both top down and bottom-up approaches:

1. A top down approach to look at Cyber as a Domain in a purely conceptual manner. We analyzed elements of the cyber domain that are unchangeable and intrinsic to the cyber domain alone and compared this to similar or comparable elements in the other domains.

   Subsequently, as a second step, we examined how these elements in other domains are addressed in terms of strategy, doctrine, requirements, and the like. Important was to examine how one can dissect the domain in a variety of ways and how to make connections with other domains. This approach was conducted by examining the academic literature on Cyber as a Domain to tap into the most recent thinking on this subject.

   The third step in this approach was to examine the role of NATO within the cyber domain. Here, we made a distinction between NATO as an enterprise and NATO as an alliance.

2. Our second approach was more bottom-up and incorporated ongoing developments with respect to the identification and formulation of cyber capabilities. NCIA is developing a framework to identify and distinguish cyber capabilities which will allow assessment of currently existing capabilities and their level of maturity and compare this to capabilities that are required or desired in the future. Taking this framework as a starting point, we have include current activities conducted by HCSS regarding the development of a framework for cyber capabilities to further refine and add to the NCIA framework, including the formulations of the dimensions to distinguish the groups of capabilities as well as of the capability groups themselves. We did this by organizing analyses sessions between NCIA and HCSS staff to combine experiences and resources.

Finally, we compared the results of both approaches to see whether and how the outcomes could show differences and gaps.

2 Cyberspace as military domain

2.1 Introduction

The consideration of any territory as a new domain in military operations is difficult per definition. While cyberspace is a concept that is nowadays widespread through societies across the globe, its actual significance and ramifications are still poorly understood. The defense domain is no exception to this. The gradual convergence of physical and digital dimensions of operations requires continuous research and understanding. Acknowledging cyberspace as a separate domain is only a first step.

As cyberspace has many dimensions, defining the term is important to converge and align thinking, communication, and analyses as well as prioritization and decision making. To start with a mutual understood set of definitions, this chapter elaborates on the concept of cyberspace and its differences to the traditional domains of the military.

2.2 Framing the Domains – General Considerations

During most of the last decade, an expanding number of member states have adopted their own national cyber security strategies and have published white papers on the subject.[3] These strategies and white papers provide numerous definitions of cyberspace and cybersecurity and the role that military organizations play in it.

While the concept of 'domain' is frequently used in defense literature, the official framing of cyber as a domain is not widely implemented. In the Joint Publications of the US Department of Defense, domain is understood as "an area under one rule; a realm."[4] This concept is frequently used but so far hardly framed, it is officially introduced by NATO and the US but not explicitly defined.

Beyond stating cyber as a domain, neither the US nor NATO have explicitly defined what cyber as a domain is. In 1995, then US Air Force Chief of Staff Gen. Ronald R. Fogleman mentioned cyber as a domain, next to previously acknowledged land, sea, and air/space domains.[5] But the United States waited until 2011 to officially introduce cyber as a domain for military operations.[6] As mentioned earlier, during the Warsaw Summit of July 2016, NATO did the same.

---

[3] CCDCOE. "Cyber Security Strategy Documents." CCDCOE, October 16, 2015. https://www.ccdcoe.org/cyber-security-strategy-documents.

[4] Ormrod, David, and Benjamin Turnbull. "The Cyber Conceptual Framework for Developing Military Doctrine." pg 284, *Defence Studies* 16, no. 3 (July 2, 2016): 270–98. doi:10.1080/14702436.2016.1187568.

[5] Gen. Ronald R. Fogleman. "Information Operations: The Fifth Dimension of Warfare." The Information Warfare Site. Accessed January 31, 2017. http://www.iwar.org.uk/iwar/resources/5th-dimension/iw.htm.

[6] *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), available at <www.defense.gov/news/d20110714cyber.pdf>

NATO now recognizes four operational domains: land, sea, air and cyberspace, with the last one added during the Warsaw summit of 2016.[7] The US Department of Defense also considers space as a domain (or more precisely an environment)[8], while NATO considers it a part of the air domain.[9]

The US Department of Defense has elaborated on those domains in various Joint Publications and it is important to have statements why differences exist and the absence of a NATO definition does matter.

The **Land domain** has been defined as "the area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals.'[10] Some unique characteristics of land domain are variations in climate and terrain, presence of non-combatants, ability to sustain operations over long time, and slower and more arduous movement when compared to air and sea.[11]

The **Maritime domain** formal definition is "the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals".[12] It is distinguished from other domains by relatively inexpensive movement only constrained by land formations, vulnerability of communication, ability to operate far from home with more flexibility when compared to air forces, and unique political and diplomatic aspects such as contradicting maritime claims by different countries. Access to maritime domain makes much of global trade possible. Domain access, deterrence, sea control power projection and maritime security are main objectives of naval forces.[13]

The **Air domain** definition is "the atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible."[14] The main characteristics of air domain capabilities are speed, range, detection, and airspace overflight. The main objective in air domain is air superiority.[15] **Space**, while recognized as a separate domain by the United States and various other nations, is considered to be a part of the air domain by NATO. Space differs from other

---

[7] CCDCOE. "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit." CCDCOE, July 21, 2016. https://www.ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.
[8] https://www.militarydictionary.org/term/space-environment
[9] http://www.airn.nato.int/page921327
[10] U.S. Department of Defense. "Joint Publication 3-31: Command and Control for Joint Land Operations." Washington, DC, February 24, 2014.
[11] U.S. Department of Defense. "Cross-Domain Synergy in Joint Operations: Planner's Guide." Washington, D.C., January 14, 2016.
[12] U.S. Department of Defense. "Joint Publication 3-32: Command and Control for Joint Maritime Operations." Washington, D.C., August 7, 2013.
[13] U.S. Department of Defense. "Cross-Domain Synergy in Joint Operations: Planner's Guide." Washington, D.C., January 14, 2016.
[14] U.S. Department of Defense. "Joint Publication 3-30: Command and Control of Joint Air Operations." Washington, D.C., February 10, 2014.
[15] U.S. Department of Defense. "Cross-Domain Synergy in Joint Operations: Planner's Guide." Washington, D.C., January 14, 2016.

domains in many regards, such as lack of borders, in both geographical and legal sense, laws of orbital mechanics relevant for satellites, the crowdedness of certain advantageous altitudes and orbital patterns, and importance of electromagnetic spectrum access. The main mission area is space force enhancement, though situational awareness, support, control and force application are also salient.[16]

Cyberspace, the newest of the domains, is defined in a number of different ways.[17] The US DoD defines it as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[18] Unique characteristics include its global and instant nature, lack of single national or international ownership as well as institutionalized collaboration and cooperation, overall low cost relative to other domains, volatility, unintended cascading effects, and the existence of four layers – physical, logical, cyber-persona, and social layer:

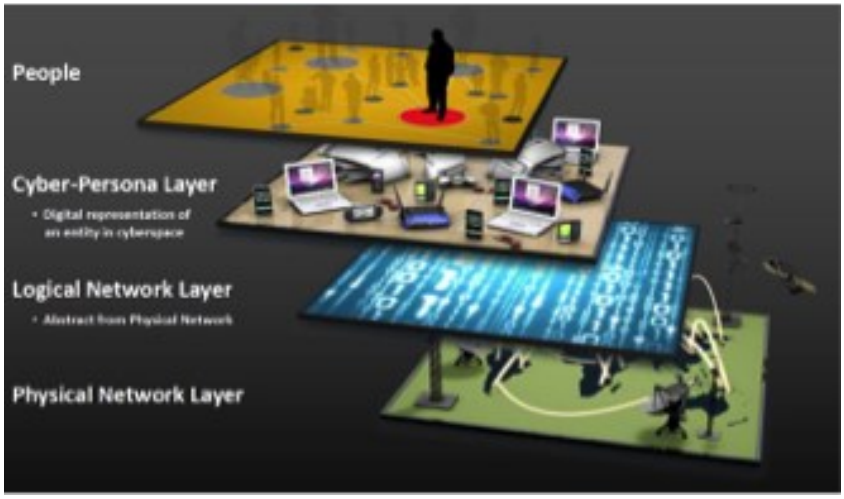


Figure 1 Four layers characterizing the Cyberspace domain

- **Physical layer** refers to all hardware – servers, computers, routers, satellite links etc. It relies to a large extent on electromagnetic spectrum, and as such is vulnerable to jamming and manipulation.
- **Logical layer** is the abstract portion of the physical layers: that is information available through Internet Protocol (IP) and URLs.
- **Cyber-persona layer** is an extension of the logical layer and represents the users, entities and organizations on the network.
- **Social layer** comprises the actors operating the ICTs and hardware.

[16] U.S. Department of Defense. "Cross-Domain Synergy in Joint Operations: Planner's Guide." Washington, D.C., January 14, 2016.
[17] For instance, see http://cyberdefinitions.newamerica.org/ for an extensive number of these definitions.
[18] U.S. Department of Defense. "Joint Publication 3-12 (R): Cyberspace Operations." Washington, D.C., February 5, 2013.

2.3 The New Domain: how does cyberspace compare to other domains?

Based on the definitions mentioned above, many countries, including the United States and NATO, consider cyberspace a domain and have operationalized it as a result. In order to determine the extent to which cyberspace can be considered a domain similar to the traditional four domains, a comparative analysis of how their immutable and variable elements coincide is required.

All domains have immutable and variable elements that are salient to them. Identifying the differences in these elements across domains, most notably those that have traditionally differentiated cyberspace from its peers, is the first step that must be taken in order to disentangle and address conceptual quagmires related to the cyberspace domain. By doing so, this chapter aims to provide an overview of the current ongoing discussions regarding the conceptualization of cyberspace as a possible domain and future formulation of cyberspace strategies and doctrines in an operational and strategic context. By first focusing on its distinguishing elements and then moving on to demonstrate how similar approaches can nevertheless be used by the way in which it is framed and thereby operationalized, the validity of its status as a domain can be better secured.

The land domain encompasses immutable elements such as urban, mountainous, jungle, or desert terrains, and takes into account physical conditions such as weather, topography, and hydrology, as well as gravity. These elements are described by their permanence and will therefore always be a constant that needs to be taken into consideration in military strategies and operations. Most often, these are natural or physical elements. Its variable elements are contingent upon these of course, and include operational and strategic factors such as civil-military relations, ground combat, drop zones, and landing zones, but also key infrastructural elements such as military bases or civilian structures. Other aspects could also be mentioned like social, cultural, religious, economical, political, energy, power structures, al influenced by human interaction. These different aspects or layers are interconnected. Variable elements can be described by their artificial nature and lack of permanence.

The maritime domain encompasses immutable physical elements such as oceans, bays, islands, or rivers, but also the weather, gravity, ocean currents, salinity, temperature, pressure, bottom topography, interconnection and the Earth's rotation (e.g. ebb and flow). It must be noted that new technological developments can, however, change the largely immutable elements into a variable. Land reclamation or land fill, for example, creates new artificial islands from oceans, lake beds, or riverbeds. In such a case, we are dealing with dynamic variables elements, and they can have a major impact. For instance, though its assertive land reclamation In the South China Sea, China enhancing its strategic and operational leverage vis-à-vis other littoral states. Nonetheless, the United Nations Convention on the Law of the Sea, clearly defines *islands* as "a naturally formed area of land, surrounded by water, which is above water at high tide", thereby excluding artificially reclaimed islands. This very own definition of an island, together with other categorizations, such as the Contiguous Zone, Territorial Sea, Exclusive Economic Zone, or the Continental Shelf, are variable elements. Their extent or the exclusive maritime rights inherent to these notions can be changed by the stroke of a pen as China pursues.

The immutable elements of the air domain are more limited than in the air and sea domains. It still includes the weather and gravity and boundless spreading of pollution, but also geomagnetic disturbances, and the Earth's rotations. The variable elements native to this domain that are

pertinent to warfare operations are more diverse, including elements such as air corridors, control zones, and air mobility components such as airlifts, airdrops, and air refueling.

Finally, the cyberspace domain encompasses many variable elements, such as the colocation center locations, the ICT infrastructures, its four layers, the physical, logical, cyber-persona, and social, as well as its three dimensions of the physical, informational, and cognitive layers. Immutable elements, however, are extremely limited. An evaluation of the differences in the warfare domains' immutable elements, both in terms of scope and numeracy, leads us to believe that cyberspace cannot be described as a segmented domain such as land or sea, but instead shows similar characteristics as an encompassing domain that is not bound by the same amount of immutable elements, nor is it easily dividable into various segments. Immutable elements of the domains are related to their physical permanence, meaning that most of the static elements will forever remain relevant during the planning of strategies and operations since they relate to the natural world. Indeed, the strategy and tactics within cyberspace, and even the domain itself, is contingent upon a physical network layer – a man-made structure, which is constituted of variables elements, and that stores and exchanges information on an electromagnetic spectrum regardless of the natural world. Cyberspace, therefore, is not even bound by constant immutable elements, such as the weather and gravity, that govern even the encompassing air domain due its artificial nature. The same traditional spatial and physical understandings therefore do not apply in the same ways to the cyberdomain.

While the air, maritime, and land domains each possess natural physical qualities and thereby necessitate related operational and strategic approaches to focus upon material indicators and factors to measure campaign success, cyberspace transcends traditional spatial warfare areas. As a man-made space, natural elements, boundaries, and limitations don't apply in the same way as they do in other domains such as land, air, maritime, or space, and normative assumptions and institutional approaches to practices and conduct are therefore less established. What ultimately arises as a result is a notion of abstractness that leads us to believe that cyberspace moves beyond the definition of an encompassing domain. While the infrastructures underpinning cyberspace can be measured and mapped, cyberspace is a mediating space that metaphorically represents the virtual landscape between and across physical networks.

For example without many physical immutable elements, cyber objectives pertaining to valuations of an **adversary's operational capabilities**, or **attack attributions** are more challenging to achieve because of their stealth nature. The achievement of anonymity through the use of proxies or encryption, inadvertent civilian action, blurred national boundaries and issues of legal jurisdiction that may arise as a result are examples of the exceptional operational or strategic factors that differentiate the cyberdomain from its peers, and drive its traditional framing as an abstract realm of operation. However as will be later demonstrated, this does not entirely prevent certain operational and strategic capabilities and concepts that are commonly applied to traditional domains from being applied to cyberspace. This is in large part due to the fact that the overall strategic capabilities remain constant across all NATO warfighting domains and certain operational factors will continue to remain highly relevant regardless of certain exceptional factors that are native to the cyberdomain.

The immutable and variable elements of each domain as discussed above are shown on the table below.

Table 1 Military Domains and its Immutable and Variable elements

Domain	Immutable elements	Variable elements

Land	• *Weather*
	• *Gravity*
	• *Terrains:*
	  ○ Urban area
	  ○ Mountainous
	  ○ Jungle
	  ○ Deserts
	  ○ …Littoral
	• Topography
	• Hydrology
	• Etc.
		• Civil-military relations (e.g. humanitarian concerns for presence of civilians)
		• Ground combat
		• Drop zones
		• Landing zones
		• Weapon systems
		• Key infrastructure
		  ○ Bases
		  ○ Civilian infrastructure
		• Etc.

Maritime	• Weather • Gravity • Oceans • Seas • Bays • Estuaries • Islands • Littorals • Rivers • Etc.	• Continental shelf • Territorial sea • Exclusive economic zone • Sea bed • Thermocline • Ports • Super captivation • Harbors • Etc.
Air	• Weather • Gravity • The earth's rotation • Geomagnetics • Etc.	• Air Corridor • Control zone • Airfield • Airhead • Etc.
Space	• Space weather • Constellations • Gravity • Constellation systems • Orbital mechanics • Etc.	• orbiting behavior • geostationary (equatorial) • geosynchronous • Lower earth orbit • polar orbit • Electromagnetics • Etc.
Cyberspace	• Data • Data transportation infrastructure • Databases • Etc.	• Colocation data center • Prevention • Detection • Attribution • Analyses • Response • Robustness • Etc.

Even though cyberspace has been implemented in the doctrines of NATO and many Member States as a domain, there still remain some dissenting views on the subject related to the aforementioned

points that differentiate it from other domains. For example, some scholars, such as Martin C. Libicki[19], reject the classification of Cyber as a Domain altogether because of its artificial and highly malleable nature and profound differences from physical domains.

Also, in an article from 2013, Frank Hoffmann and Michael C. Davies urge for a renewed conceptual framework that goes beyond the four physical domains by introducing the cross-cutting and all-encompassing human domain, e.g. human interactions across all domains, which they believe is underrepresented in national military doctrines or strategies.[20] They claim that cyberspace is connected to all four physical domains,[21] as do of David Ormrod and Benjamin Turnbull.[22]

The latter offer their own nested model, in which they vertically distinguish between three domains of overall national security domain, namely political, economic and military domains, as well as horizontally between physical and virtual domains, and claim that domains can be nested within each other.

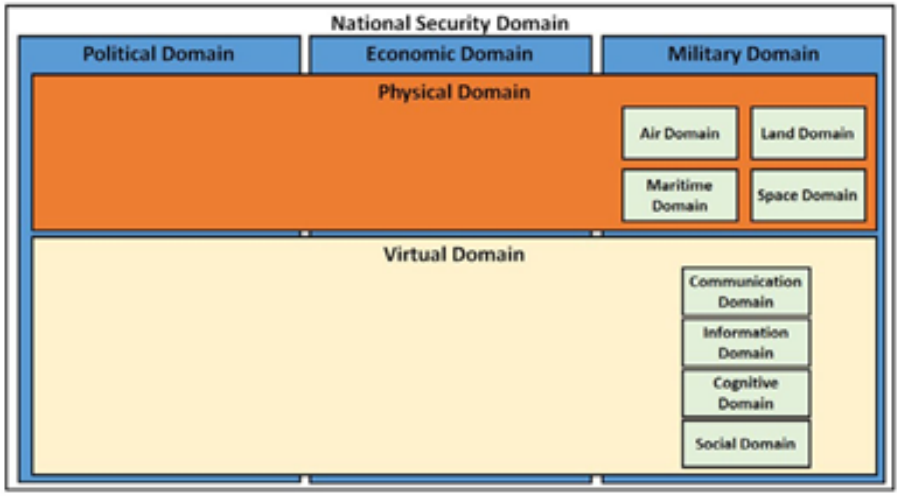


Figure 2 The military domains as part of the overall broader and non-exclusive national security domain[23]

In their framework, they identify the air, land, sea, and space domain as the physical domains just as Hoffman and Davies, but separate them from the virtual domain, which comprises the communication, information, cognitive and social domain. All four reject the assertion of cyberspace as a conventional domain on the basis that the conceptualization would create boundaries which are not representative of the complexities of cyberspace. Moreover, it would insufficiently describe the

[19] Libicki, Martin C. "Cyberspace Is Not a Warfighting Domain." ISJLP 8 (2012): 321.
[20] Hoffman, Frank, and Michael C. Davies. "Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework?" *Journal Article | Jun* 10, no. 1 (2013): 30am.
[21] The authors also distinguish between physical (infrastructure such as computers and links) and cognitive (ideas and imagery) elements of cyberspace.
[22] Ormrod, David, and Benjamin Turnbull. "The Cyber Conceptual Framework for Developing Military Doctrine." *Defence Studies* 16, no. 3 (July 2, 2016): 270–98. doi:10.1080/14702436.2016.1187568.
[23] Ibid.

interactions between technology, society, people, situational awareness and battlefield effects. They instead refer to cyberspace as an environment that has both physical and virtual elements, which should be considered across all conventional battlespace domains and at all levels (strategic, operational and tactical). Neither, however, dismiss the importance of cyberspace for achieving success in the military sphere.

A common thread is the categorization of cyberspace as an 'abstract,' or part of a 'virtual' domain, with unprecedented unique attributes, in contrast to the conventional land, sea, and air domains. Similarly, the importance of cyberspace to all other domains as means of distributing information is emphasized by all. However from an operational perspective it remains clear that the added value of including cyberspace as a warfighting domain is identical to those of traditional domains, as despite its exceptional differences it remains – from an operational perspective – comparable in terms of approaches and outcomes. While the conclusions of Hoffman and Davies (2013) are certainly valid in its depiction of cyberspace as a facilitative environment that brings added value to operations carried out in the traditional domains, by bridging concepts such as that of an operational "high ground" to cyberspace (see Section 2.4.3), it can be seen that the same operational approaches can hold true after taking into consideration the sensitivities that are demanded by cyberspace.

Furthermore, the operational tasks and outcomes that come as a result of the way that these domains are utilized can also demonstrate cyberspace's applicability as a warfighting domain. Much like in air, land, and the maritime domains, strategic capabilities such as command, control, and communications (C3), survivability and force protection, and effective engagement processes are equally integral – and more importantly – equally applicable to the cyber domain. As a result, while taking note of the unique aspects of cyberspace when compared to land, sea, air and space, we conclude that it can, and should be considered to be a military domain, as NATO as well as many countries already do, and due to its critical importance, a priority should be given to improving its relevant defense and maintenance tasks as a result.

2.4 Unique attributes of cyberspace: sources of insecurity

Cyberspace is fundamentally different from the physical domains, and as such some concepts like the high ground and borders are conceptualized differently in theory and as such their practice varies as well. Here is an overview of some notable differences.

Table 2 Differences between cyberspace and other domains as articulated by Brades (2013)

Characteristic	Cyberspace Domain	Traditional Domains
Resources	• Inexpensive relative US air, land and sea • Human capital-driven	• Limited to nations with significant financial resources • Industrial-based assets
Physical	• Artificial construct, permeable virtual boundaries • Multi-use environment (government, military, commercial) • Distributed, dynamic and non-linear	• Exists naturally, discrete physical boundaries • Multi-use environment (government, military, commercial)
Actors	• Ambiguous • From nation-states to individuals to criminal organizations to commercial entities	• Identity of adversary usually known
Effects	• Global in nature • Non-Kinetic or Kinetic • Collateral damage on 2nd/3rd order effects potentially global	• Usually regionally focused (Space is exception) • Usually Kinetic (EW exception) • Collateral damage limited to active battlespace
Authorities for Offensive Action	• Elevated • Evolving ROE	• Local • Establish ROE
Intelligence Support	• Requires knowledge of adversary capabilities and intent • Compressed timeline ("net" speed) • Attribution is challenging	• Requires knowledge of adversary capabilities and intent

3 Analytical Capability Framework for Cyberspace

3.1 Introduction

Beyond defining and distinguishing the operational domains of land, sea, air, and cyberspace, the possibility of linking these domains to each other is equally relevant. This possibility of linking will facilitate the understanding of how different capabilities in each domain can reinforce the overall effectiveness of operations and can align active cooperation among forces of different domains.[24] This process of linking is supported by the use of analytical frameworks.

3.2 What is an Analytical Framework?

An analytical framework is a construct that can be used for both communication and decision making and helps to answer questions by comparing and collecting data, conducting gap or prioritization analyses, pattern recognition, consistency checks, etc. There are analytical frameworks for all kind of applications, businesses and processes. These analytical frameworks are often specific and tailored to the user's intended aims and/or functions.

3.2.1 How to analyze the capabilities the NATO Strategic Commands need?

After declaring Cyberspace the fourth NATO domain, the question arises: what are NATO Strategic Commands capable of, and what does this declaration mean for the overall strategic functions of NATO Strategic Commands, its Member States and its cyberspace capabilities?

3.2.2 Current NATO Cyberspace Analytical framework

Currently, NATO Communications and Information Agency (NCIA) already has an analytical framework in place. This framework takes a top down perspective, has one dimension and consists of various elements in an hierarchical system. However, the focus is specifically concentrated on CIS security and as a result does not take into account a broader view of cyberspace, and therefore cannot be easily transposed to fit any of the other domains. As a result, while it does partially address specific strategic functions, the analytical framework cannot be applied to NATO's other military domains or practically bridge and make capabilities comparable or additional to the other domains. It also cannot be applied to analyze NATO's interactions and collaboration between the military and civil domains or with its Member States.[25] While it is possible to map capabilities (existing, wanted or missing) with this framework, it is however, not possible to prioritize the importance of capabilities and to understand the linkages between different capabilities and domains. While it is clear that the existing framework provides a comprehensive approach to CIS security, it cannot be applied in pursuit of goals that branch outside of this area. This framework is therefore in need of being expanded upon or otherwise supplemented due to NATO's more

[24] U.S. Department of Defense. "Cross-Domain Synergy in Joint Operations: Planner's Guide." Washington, D.C., January 14, 2016. and Palazzo, Albert, and David P. McClain III. "Multi-Domain Battle: A New Concept for Land Forces." War on the Rocks, September 15, 2016. https://warontherocks.com/2016/09/multi-domain-battle-a-new-concept-for-land-forces/.

[25] Ormrod, David, and Benjamin Turnbull. "The Cyber Conceptual Framework for Developing Military Doctrine." *Defence Studies* 16, no. 3 (July 2, 2016): 270–98. doi:10.1080/14702436.2016.1187568.

expansive perspective taken towards cyber operations and strategy as a result of its designation of Cyberspace as a distinctive warfighting domain.

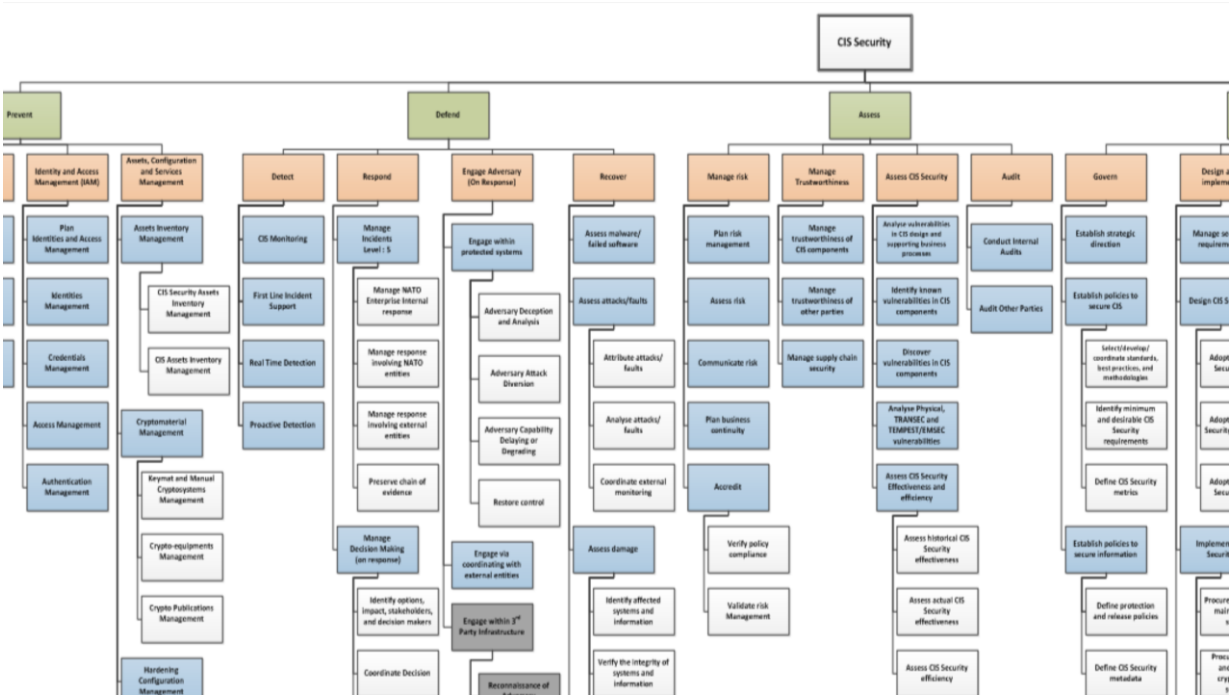


Figure 3 A portion of NATO's current cyber capability framework (cropped)

For this study, it was deemed necessary to combine the following requirements in an analytical framework. Through these requirements, it should be possible to use the analytical framework for communication, analysis and decision-making purposes. With these in mind, the produced analytical framework should therefore be able to:

1. Apply within the cyberdomain;
2. Apply across all other military domains;
3. Apply within a domain for specific strategic functions;
4. Apply between the military and civil domains;
5. Apply between NATO and its member states;
6. Map capabilities and capacities (existing, wanted or missing);
7. Prioritize the importance of capabilities and capacities;
8. Help understand the linkages between different capabilities and domains.

With these identified goals, the produced analytical framework will be able to give an effective account of possible further points of expansion for NATO's existing security framework, which has been effective for the development and maintenance of relevant CIS protection tasks. This conceptual framework is therefore a suitable tool to use because the operationalization of the cyberspace domain requires a more expansive outlook on cyber tasks in order to develop NATO capabilities responsibly and effectively. This is exemplified in its focus on strategic capabilities and strategic functions, and its potential to be built upon using further levels of assessment – which can also be integrated into the framework support by software tools like Tableau – gives it even more value for the more comprehensive considerations that will be required in future NATO cyber operations and strategies.

3.2.3 What is a Strategic Function

A prior study for the Netherlands Ministry of Defense was used to construct an analytical framework. Part of the framework were Strategic Functions. Strategic functions were formulated in a nationwide study called the 'Verkenningen 2010, Houvast voor de krijgsmacht van de toekomst' from 2010[26] and the Netherlands Defence Doctrine 2013.[27]

Strategic functions are defined as the top level activities a military organization should be capable of and through which desired effects can be generated.

Figure 4 Seven Strategic Functions of which parts are a responsibility for NATO. Some functions like Intervene (offensive actions) are up to now reserved for the Member States.

For this analytical framework these strategic function definitions were re-used. The strategic functions and their definitions are as follows:

1. **Anticipation**: Preparing for foreseen and unforeseen developments and incidents that may affect the interests of NATO and its member states;
2. **Prevention**: Active steps intended to prevent a threat from occurring that is contrary to the interests of NATO and its member states or the international rule of law;
3. **Deterrence**: Discouraging activities that conflict with the interests of NATO and its member states or the international rule of law by upholding the prospect of retaliatory measures;
4. **Protection**: Protecting and, if necessary, defending the territory and residents of NATO member states and property registered within NATO member state territory;

[26] Ministerie van Defensie. "Verkenningen 2010, Houvast Voor de Krijgsmacht van de Toekomst," 2010.
[27] Ministerie van Defensie. "Netherlands Defence Doctrine," 2013.

5. **Intervention**: Enforcing a change in the behavior of one or more parties that threaten the interests of NATO or its member states or the international rule of law;
6. **Stabilization**: Establishing security in a current or former conflict zone to achieve political stability and economic and social development;
7. **Normalization**: Restoring normal living conditions after a conflict or disaster.

3.2.4 What is a Strategic Capability?

To fulfill a strategic function, a military organization needs to be capable of doing things. To that end the syntax of a capability may be defined according to the following format:

"*The ability to* … [do something] … with… [an intended effect and/or outcome]"

Examples:

- The ability to cooperate long-term with law enforcement institutions, private sector and CI providers to exchange expertise and information;
- The ability to estimate various levels of danger from cyberspace to implement adequate protection measures;
- The ability to prepare flexible diplomatic and C3 structures capable of engaging in cyber dialogue with non-NATO nations.

The following generic or strategic capabilities are recognized in our analytical framework, and can be applied to all domains. While perhaps not an exhaustive list (as more defined strategic capabilities can be identified on a domain-specific level), these capabilities provide a comprehensive overview of the competences that will be required for the planning and execution of virtually any military operation. Their cross-domain validity ensures that the method of analysis can be equally beneficial for the development of future operational and strategic objectives across all NATO operational domains.

The strategic capabilities and their definitions are as follows:

1. **Effective command, control and communications (C3)**: The capability to provide effective direction and steering for units and staffs in order to achieve the set objective(s);
2. **Effective engagement:** The capability of deploying personnel and weapons systems throughout the entire spectrum of force, thus damaging the operational capability of the other party or parties;
3. **Timely force availability:** The capacity to build up and support a sufficient and effective operational capability within a given response time, thus allowing the assigned tasks to be carried out;
4. **Deployability and mobility:** The capability to relocate an asset within a set time period to the required location and then to perform a task while retaining military capability;

5. **Logistics sustainability:**[28] The capability to provide, manage, care for and maintain as well as supply and remove personnel and equipment to and from units and staffs, in order to enable them to conduct their assignment;
6. **Effective intelligence:** The timely collection, processing and dissemination of effective information in order to be able to anticipate and where necessary respond to any situation in which the security of own or Allied troops is compromised;
7. **Survivability and force protection:** The capability to retain one's own military capability by limiting the effects of activities of others, including the deployment of lethal and non-lethal weapons, and by ensuring freedom of action and deployment of weapons.

3.2.5 What is a Cyberspace Capability

Cyberspace is a combination of networks of information technology infrastructures (including hardware such as: computers, cables, buildings, routers, switches, servers, exchanges, data warehouses, etc.) and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[29]

Within the military cyberdomain, information, technology infrastructures and data software etc., are used for two purposes, namely:

1. Cyberspace capabilities that enhance the capabilities in the other domains (air, land and sea);
2. Independent or standalone cyber capabilities that are used only in the cyberdomain.

Taking an example cyber capability from the aforementioned study carried out for the Netherlands Ministry of Defence, *Forward Cyber Defence* is defined as "the ability to send cyber military advisory teams to strengthen prevention capabilities." This capability fits to both a strategic function (*Prevention*) and a strategic capability (*Timely Force Availability*) and is both more clearly defined and linked to an intended outcome that is in line with organizational strategic functions and capabilities.

3.3 Proposed extended Cyberspace Analytical framework

3.3.1 Overview

A new concept for an analytical framework has been proposed to better represent the interconnectedness of the different capabilities within and across the domains and can be used to extend NATO's existing Cyber analytical framework. This new analytical framework developed for the cyberspace domain has two dimensions, namely **strategic functions** (here shown as columns) and **strategic capabilities** (here shown as rows), while the cells in the matrix provide space in which

[28] While at face level it can be assumed that logistics issues (and to a lesser extent those regarding deployability and mobility) do not apply to the cyber domain. However cyber capabilities related to these strategic capabilities exist in the form of patch and hotfix distributions, deployment of cyber advisory teams, and hardware logistics for example. Thus it cannot be assumed that the aspect of immediacy innate to cyberspace reduces the need of logistical, mobility or deployment strategic capabilities.

[29] https://www.militarydictionary.org/term/cyberspace

operational and strategic cyber capabilities, or use cases[30], developed by HCSS, can be shown. The current figure shows the number of cyber capabilities (including sub-capabilities) and use cases per every strategic function and capability combination. The produced use cases fit to cover each cell of the analytical framework, and were developed in cooperation with Dutch defense officials and as such are more specified examples of cyber capabilities that are of value for cyber operations. They are not representative of a complete set of cyber capabilities however, and are best used as examples.

Through the plotting of strategic functions and strategic capabilities on two separate axes, a framework is developed in which each cell represents a space in which the requirements for NATO to fulfil a certain function may be positioned. This comes in the form of a cyber capability – or – a use case.

	Anticipation	Prevention	Stabilisation	Intervention	Normalisation	Deterrence	Protection
Timely Force Availability							
Effective C3							
Effective Intelligence							
Effective Engagement							
Mobility/ Deployability							
Survivability and Force Protection							
Logisitics Sustainment							

Figure 5 Strategic Function/Strategic Capability matrix structure of the proposed analytical framework

To test the above described new analytical framework and evaluate its value for practical application, the framework was tested using the combination of capabilities found in the current NATO framework (see Figure 3) in addition to an extensive set (one for each matrix cell, denoting a distinctive strategic function and capability combination) of use cases from an earlier analysis carried out for the Dutch Ministry of Defense. The findings of this analysis are presented in Figure 6, which shows the number of specific capabilities of the NATO framework on a matrix with the axes being

[30] The term "use case" is used when describing cyber capabilities in the context of the HCSS cyber capability board game produced for the Netherlands Ministry of Defence. By referring to each capability as such rather than as "cards" for example), it can be better understood as a single case that could be placed in its position on the matrix rather than a complete blanket capability. This can trigger further granular analysis considering what other capabilities as "use cases" can potentially be placed at its location. Thus here, use cases refer to HCSS example cyber capabilities taken from our prior study, whereas capabilities refer to those from NATO.

strategic functions and strategic capabilities of the HCSS analytical framework. A multi-level gap analysis (investigating the distribution of NATO cyber capabilities at all levels, ranging from top-level capabilities to sub-capabilities) was also performed based upon the results (see Section 3.4).

	Strategic Function						
Strategic Capability	Anticipation	Prevention	Deterrence	Protection	Intervention	Stabilisation	Normalisation
Effective C3	56	46	29	53	43	57	55
Effective Engagement	37	34	26	45	39	47	47
Timely Force Availability	37	25	16	31	27	42	42
Deployability and mobility	38	22	19	33	28	43	43
Effective Intelligence	61	58	39	54	39	67	50
Logistics Sustainability	42	28	21	34	28	46	43
Survivability and Force Protection	56	45	38	52	33	47	41

N
16 67

Figure 6 The analytical framework combining Strategic Functions and Strategic Capabilities.

Figure 6 shows that there are a divergence in numbers of specific capabilities per different strategic functions and strategic capabilities. For example, there are less capabilities for serving the functions of deterrence and intervention than the other five strategic functions. Effective intelligence is the strategic function with the most specific cyber capabilities assigned to it. This is indicative of the division of tasks assigned to NATO compared to the Member States, and of the unique characteristics of cyberspace.

In addition to our plotting of NATO's cyber capabilities on the proposed framework, we also performed a back testing analysis in order to more concretely define the strengths and limitations of NATO's existing framework. This was done by plotting the specialized use cases on NATO's current framework. The findings of the back testing generally confirmed that NATO's current conceptual framework is in need of further expansion in order to recognize the greater role that cyber capabilities have taken as a result of NATO's recognition of cyberspace as a warfighting domain. While CIS security will remain an integral component to the further development of NATO's cyber capabilities, a number of new factors will likely need to be taken into consideration in future decision making processes. For this reason, more effective solutions are needed to orient NATO's existing cyber capabilities towards its strategic functions and align them with those of its other domains.

The produced sheet (See Appendix 1. Full visuals) plots the HCSS use cases along NATO's existing CIS analytical framework. The HCSS use cases are very specific and are examples of cases that can come as a result of more refined, granular analysis intending to develop explicit cyber assets, activities, and processes. They also can provide a more realistic view of cyber capabilities due to their consideration of inter-sectoral interactions (such as with the military or civil sectors). By plotting them against NATO's current framework, we can more easily identify points for further improvement by showing the limitations of using such a specific framework for more refined use cases.

Overall we can see that the existing framework can be updated effectively to become more comprehensive due to the acknowledgment of cyber as a domain rather than as a set of systems and processes that primarily facilitate functions and capabilities in other domains. Both our set of example use cases and those provided by NATO can be fit to our proposed analytical framework, demonstrating its suitability for both top- and bottom-level use cases.

We believe that our proposed analytical framework is an effective tool to determine further points of improvement for NATO's existing analytical framework, which focuses on CIS security, by specifically

broadening applicability to suit a wider set of operational and strategic goals. Our framework plots NATO cyber capabilities on an input-output matrix based upon its strategic functions and strategic capabilities. The framework of our matrix enables it to be applied to other domains as well, meaning that similar analyses can be carried out to identify and develop NATO capabilities on Sea, Air, and Land as well. This ensures a consistent approach to relating assets, activities, and processes to organizational functions and capabilities across all domains.

Overall, the two analytical frameworks should be recognized as separate, distinctive tools that can be used to pursue two equally separate, distinctive goals. The existing CIS security framework remains effective in its applications towards CIS security, and the proposed analytical framework can be used to understand the relevant capabilities that are needed to carry out cyberspace operations. It can therefore be used to develop capabilities along these lines, and can drive the development of further extensions to the NATO analytical framework to provide a more comprehensive overview of operationalization of the Cyber domain. In addition to those use cases already provided to the Netherlands Ministry of Defence (see Appendix 2. HCSS set of example use cases), the production of additional cyber capabilities matching specific fields on the Strategic Function/Strategic Capability framework can also be used as seed ideas for the further expansion of NATO's current analytical framework.

3.3.2 NATO Capability Plotting Outcomes

The analytical framework was tested using a physical card (each reflecting a given use case) game version allowing us to plot each capability on a planar surface in the form of a board game. The results were captured in Microsoft Excel. Additional categories were also provided in this Excel. For example including offense/defense or flexible, private partnerships, Member State partnerships etc. These results are available and are provided as a separate deliverable (Excel files). We combined and integrated the NATO set of capabilities with both the different levels of breakdowns (see Figure 3, down to three sub-levels) and with the example use cases that had been developed for the Netherlands Ministry of Defence to show differences, similarities etc.[31] After doing so it was possible to analyze gaps and differences as well as similarities in the frameworks and subsequent capabilities.

By visualizing the plotting results of the conceptual framework, a number of conclusions can be made. Several distinctions differentiate these visualizations from one another, with each having a different value for the analysis. The produced visualizations are evaluated below on the basis of how they demonstrate the expanded utility and applicatory values of our conceptual framework.

[31] The visuals and their related analyses found within this text will include the cyber tasks created for the Dutch Ministry of Defense unless otherwise stated.

Figure 7 Our interactive cyber strategic capability board game produced for the Dutch Ministry of Defence

Specific capabilities by strategic functions and strategic capabilities

Figure 8 and Figure 9 show the breakdown of specific cyber capabilities as operationalized by NATO in the HCSS analytical framework, first shown by strategic functions and then by strategic capabilities. As both graphs are large, only cropped snapshots are shown here, with the full visuals available as separate images and also in the appendix. Those visuals further illustrate the point that was made earlier, namely that the strategic functions deterrence and intervention have less tasks assigned to them than the other five.

Main capability	Level	Specific capability	Anticipation	Prevention	Deterrence	Protection	Intervention	Stabilisation	Normalisation
Analyse	Main task	Analyse	■	■				■	
	Sub-task 1	CIS Dependencies Analysis	■	■				■	
		Operational Value Analysis	■	■				■	
		Threat Information Analysis	■	■				■	
Assess CIS security	Main task	Assess CIS security	■						
	Sub-task 1	Analyse Physical, TRANSEC and TEMPE..	■						
		Assess CIS Security Effectiveness and e..	■						
		Assess vulnerabilities in CIS design and..	■						
		Discover vulnerabilities in CIS compone..	■						
		Identify known vulnerabilities in CIS co..	■						
	Sub-task 2	Assess actual CIS Security effectiveness	■						
		Assess CIS Security efficiency	■						
		Assess historical CIS Security effective..	■						
Audit	Main task	Audit	■	■					
	Sub-task 1	Audit Other Parties	■	■					
		Conduct Internal Audits	■	■					
CIS Protection	Main task	CIS Protection	■	■	■	■	■	■	
	Sub-task 1	Boundary Protection	■	■	■	■			
		Endpoint Protection	■	■	■	■			
		Network Protection	■	■	■	■			
		Physical and personal security	■	■	■	■			
Collect	Main task	Collect	■	■	■	■	■	■	■
	Sub-task 1	CIS Information Collection	■	■				■	
		Consolidated Repository Management	■	■				■	
		Operational Information Collection	■	■				■	
		Reference Information Collection	■	■				■	
		Threat Information Collection	■	■				■	
	Sub-task 2	Intelligence Collection	■	■				■	
		Non-malicious Threat Information Colle..	■	■				■	
Data Protection	Main task	Data Protection		■	■	■		■	
	Sub-task 1	Data Wiping		■	■			■	
		Information Redaction		■	■			■	
		Object Level Protection		■	■	■		■	

Figure 8 Specific capabilities by strategic function (cropped)

Figure 9 Specific capabilities by strategic capabilities (cropped)[32]

Specific capabilities by strategic function

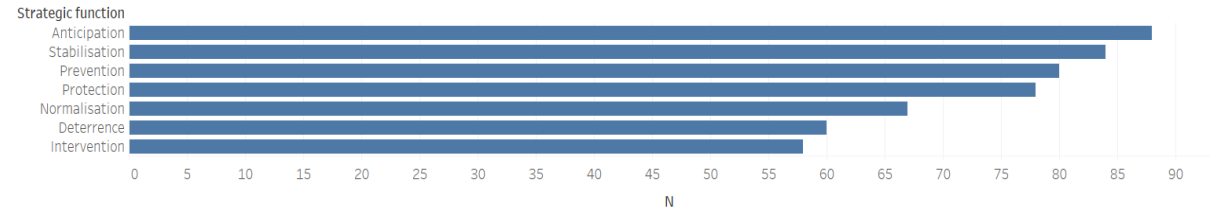


Figure 10 Specific capabilities by Strategic Functions

Figure 10 shows the total number of tasks that fall under each function according to our conceptual framework's classification of cyber capabilities. Here we can see that NATO's current cyber capabilities are most focused on strengthening its anticipatory functions. On the other hand, its current cyber capabilities are least focused on strengthening its intervention and deterrence functions. In order to have a more complete cyber capability package, it would be recommended that NATO would work on filling the gaps for those functions, or work with the member states to make sure the capabilities needed exist.

[32] The visualizations were made using the data visualization software Tableau and are available as a separate deliverable (in the form of Tableau files as well as high quality images). These can be opened and viewed via the usage of a free Tableau software product, Tableau Reader. Images of these visualizations can be found in the Appendix 1. Full visuals.

Specific capabilities by strategic capability

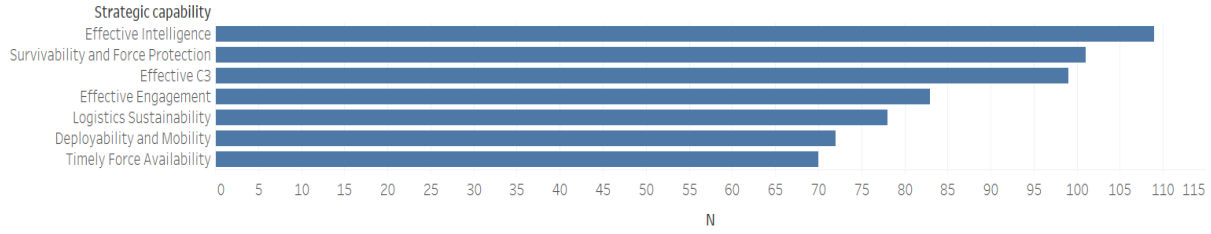


Figure 11 Specific capabilities by strategic capabilities

Figure 11 shows the number of NATO's specific capabilities by strategic capabilities as operationalized by HCSS. We see that the strategic capability with the highest number of specific capabilities is effective intelligence, which is reasonable considering the fact that much of the information exchange in today's world happens in cyberspace. For some material strategic capabilities, such as timely force availability, and deployability and mobility, the number of cyber capabilities is lower, also in line with its characteristics.

Ranking NATO's current capabilities by strategic capabilities and functions

Figure 12 shows how current NATO cyberspace capabilities are distributed across the HCSS framework's strategic function and strategic capability fields. Here we can see that unlike the cyber capabilities created for the Dutch Ministry of Defense, NATO's current cyber capabilities have broader utility across multiple dimensions. The most broadly-applicable cyber capabilities here are regarding adopting and developing various security measures as well as information sharing with both external parties and inside the organization.

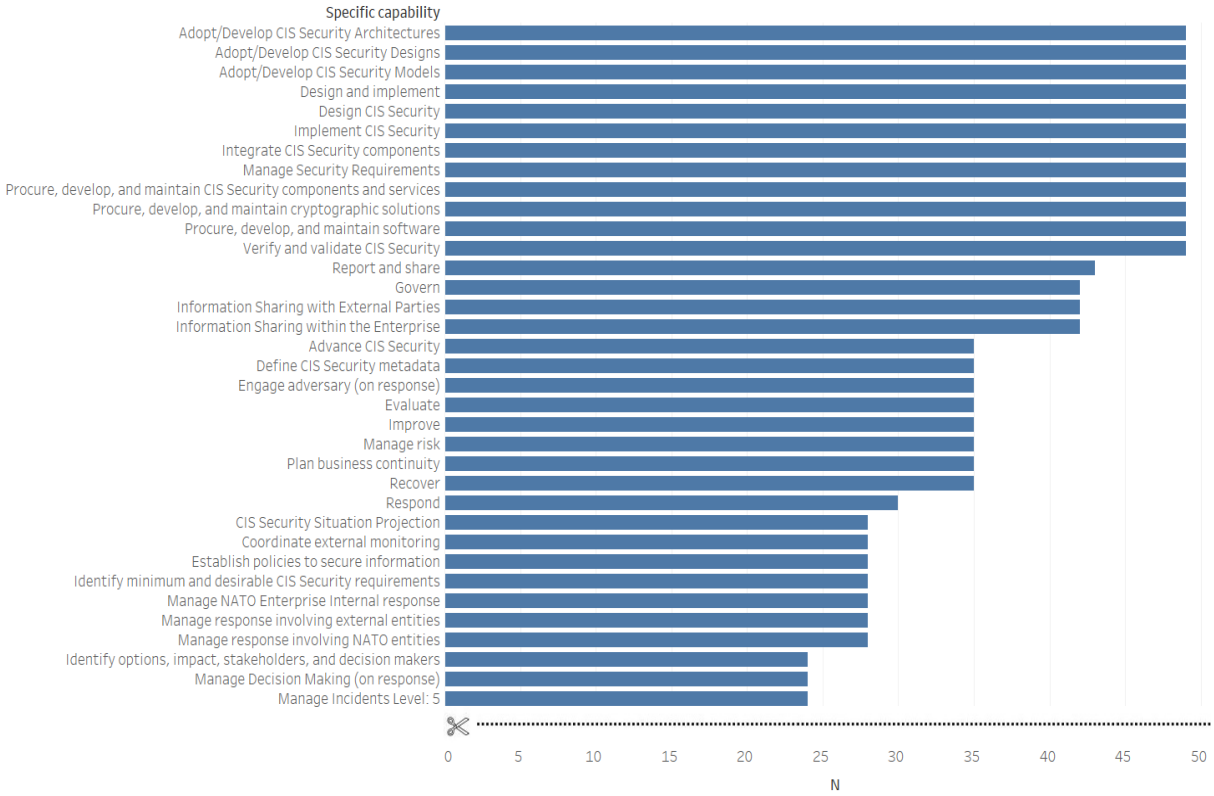


Figure 12 Ranking NATO's current capabilities by strategic capabilities and strategic functions (cropped)

Structure by defense and offence

This visualization shows the spread of NATO cyber tasks according to their offensive or defensive value to NATO strategies and operations. Here we can once again see that NATO's current cyber capabilities largely have value for its defensive strategies and operations. Here the data is broken down, and we can see (perhaps expectedly) that NATO's offensive cyber capabilities are largely found under the intervention and protection functions, the latter due to its rule of cyber engagement being largely confined to the realm of retaliation.

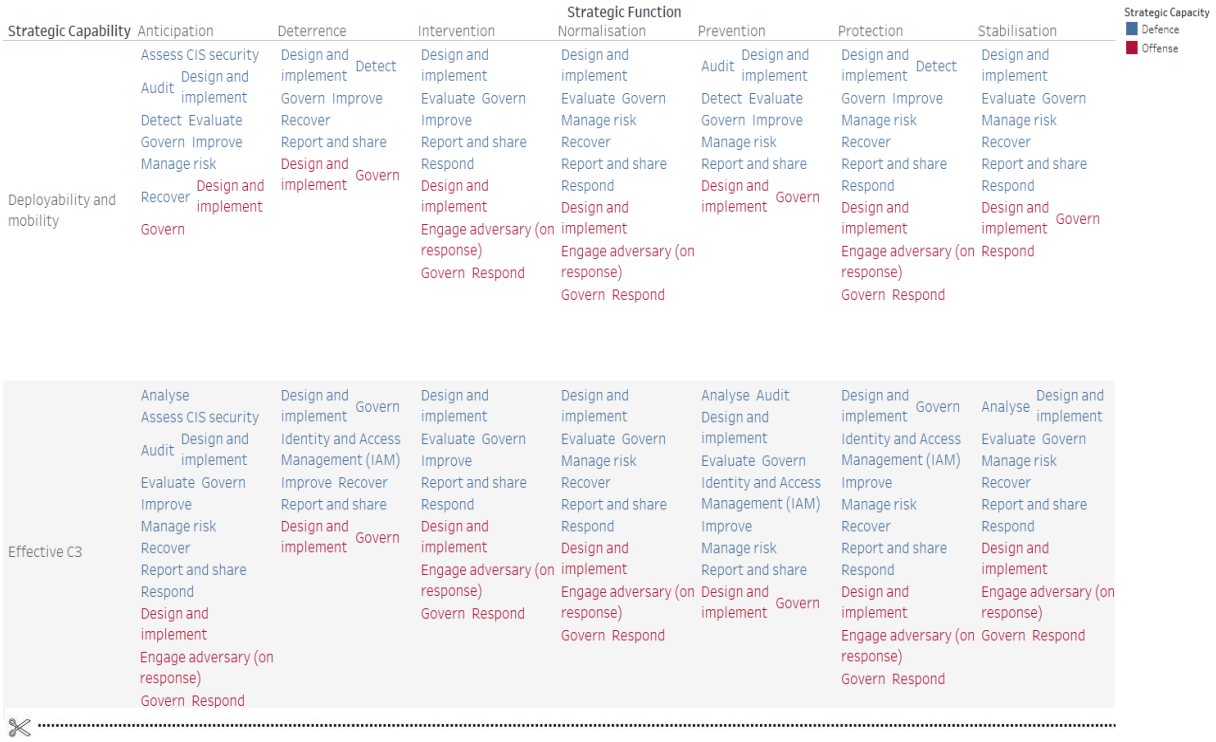


Figure 13 Structure by defence and offense (cropped)

Structure by non-state partnerships

This visualization shows the spread of NATO cyber capabilities and displays them by color on the basis of whether they could potentially involve non-state actors. The distribution here is fairly equal, and shows the high degree of involvement non-state actors may have in future NATO cyber capabilities and operations. Also clear is the degree of ambiguity in a number of capabilities as defined by NATO. For these, it is unclear whether or not non-state involvement is crucial, or otherwise possible.

Figure 14 confirms that the current set of NATO cyber capabilities leave ample room for increased partnerships with non-state actors. While internal competencies related to CIS protection remains a NATO core competence, cyber capabilities such as *Manage risk*, *Report and share*, or *Improve* all could potentially be expanded to involve non-state actors in order to increase their reach and effectiveness. The results of our plotting analysis along these lines lead us to recommend that NATO might consider developing its existing strategic partnerships within the private sector in order to improve their cyber strategic capabilities.

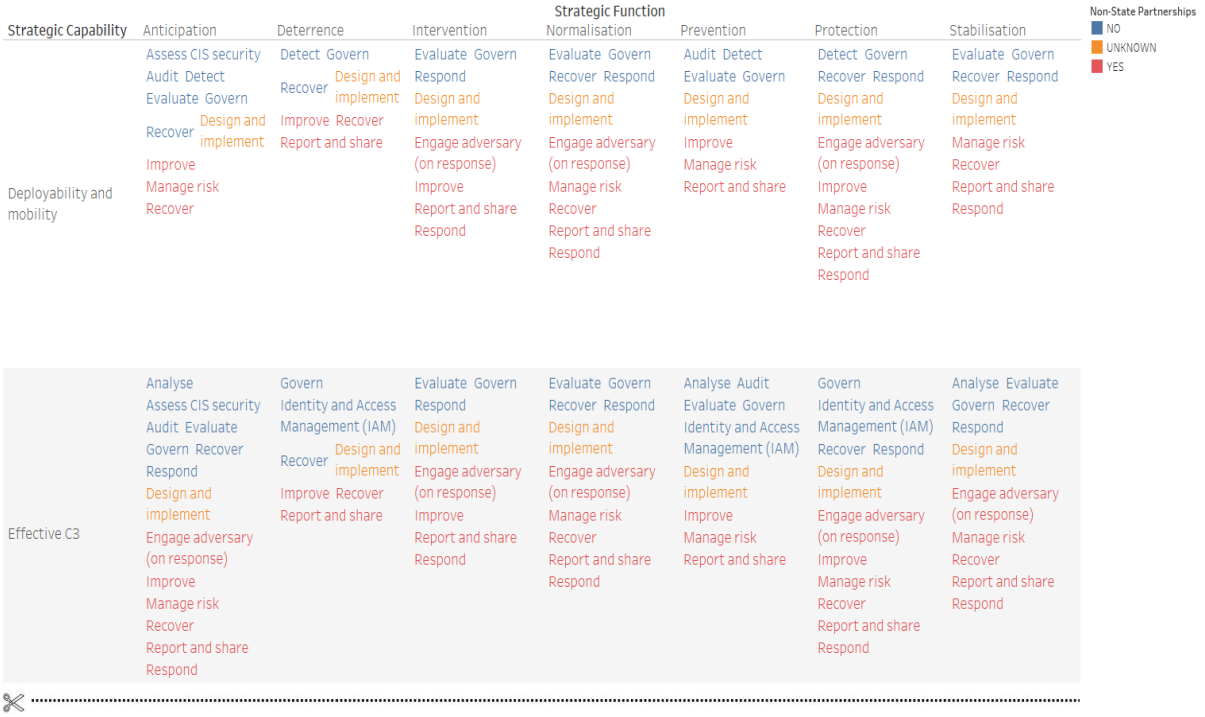


Figure 14 Structure by non-state partnerships (cropped)

3.4 Multi-Level Gap Analysis

After categorizing NATO current cyberspace capabilities along the structure of the HCSS analytical framework,[33] coverage gaps in the matrix elements can be seen on various capability levels.[34] While the provided set of NATO CIS current capabilities is extensive, when both summating the data and investigating them at different variable levels we can uncover areas in need of further attention. Following are the results of the gap analysis as well as a number of accompany visuals that demonstrate the distribution of the use cases across the Strategic Function/Strategic Capability matrix.

[33] Note that for the following analysis we used the use case classifications of NCIA (provided by the project sponsor) to ensure one distinctive line of analysis and also to ensure the validity of our conclusions.

[34] The term "levels" here indicate the capability's degree of subordination according to NATO's CIS Security Capability Breakdown document, in which capabilities are broken down into three categorical sets (e.g. A.1 *Prevent*, A.1.1 *CIS Protection*, A.1.1.1 *Boundary Protection*).

NATO CIS Security Capability Use Case Breakdown Plotted by Function/Capability (All levels)

	Strategic function						
Strategic Capability	Anticipation	Deterrence	Intervention	Normalisation	Prevention	Protection	Stabilisation
Deployability and mobility	38	19	28	43	22	33	43
Effective C3	56	29	43	55	46	53	57
Effective engagement	37	26	39	47	34	45	47
Effective Intelligence	61	39	39	50	58	54	67
Logistics sustainability	42	21	28	43	28	34	46
Survivability and Force Protection	56	38	33	41	45	52	47
Timely Force Availability	37	16	27	42	25	31	42

Figure 15 Full set of NATO CIS security capabilities plotted on Strategic Function/Strategic Capability Matrix

Figure 15 shows that capabilities at all levels provide basic coverage across all matrix cells. The distribution of cyber capabilities however remains disproportionately allocated. Most noticeable within this figure is the limited number of cyber capabilities that provide value for NATO's deterrence function. Furthermore, the allocation of cyber tasks along its strategic capabilities also are uneven, with significantly more cyber capabilities falling within the *Effective C3*, *Effective intelligence*, *Sustainability and Force Protection* strategic capability categories. The unequal allocation of cyber capabilities in these cases might mean that NATO will be less effective in its *Deterrence* abilities, and its *Deployability and mobility, Effective engagement, Logistics sustainability,* and *Timely Force Availability* strategic capabilities are not as effective as they could be. This visual includes consideration of the NATO *Design & Implement* capability, which is excluded in other visuals due to its wide categorization range.

NATO CIS Security Capability Use Case Breakdown Plotted by Function/Capability (All levels, excluding Design & Implement)

Strategic Capability	Strategic function: Anticipation	Deterrence	Intervention	Normalisation	Prevention	Protection	Stabilisation
Deployability and mobility	26	7	16	31	10	21	31
Effective C3	44	17	31	43	34	41	45
Effective engagement	25	14	27	35	22	33	35
Effective Intelligence	49	27	27	38	46	42	55
Logistics sustainability	30	9	16	31	16	22	34
Survivability and Force Protection	44	26	21	29	33	40	35
Timely Force Availability	25	4	15	30	13	19	30

Figure 16 Full set of NATO CIS security use cases plotted on Strategic Function/Strategic Capability Matrix excluding Design and Implement use case and its related sub-capabilities

Figure 16 shows the distribution of NATO cyber capabilities at all levels excluding the NATO *Design & Implement* capability, which has a wide categorization range. When excluding the capability along with its related sub-capabilities the distribution remains the same. This visual is included for reference value.

NATO CIS Security Capability Use Case Breakdown Plotted by Function/Capability (Top level, excluding Design & Implement)

Strategic Capability	Strategic function: Anticipation	Deterrence	Intervention	Normalisation	Prevention	Protection	Stabilisation
Deployability and mobility	5		2	1	2	2	2
Effective C3	7	2	3	3	5	5	4
Effective engagement	4		2	1	2	2	2
Effective Intelligence	8	3	3	2	7	5	5
Logistics sustainability	5		2	1	2	2	2
Survivability and Force Protection	7	2	2	1	4	4	4
Timely Force Availability	5		2	1	2	2	2

Figure 17: NATO CIS security top-level capabilities plotted on Strategic Function/Strategic Capability Matrix excluding Design and Implement capability

Figure 17 shows largely the same plotting distribution as Figure 18, however the degree of disproportionality is perhaps more striking at the displayed top level. Here, there are several matrix cells within the Deterrence Strategic Function column that are not covered by any cyber capabilities. While this view does not take further sub-capabilities past the top level into account (which do

provide adequate coverage as evidenced by Figure 18) the results reveal the need for NATO to develop its Deterrence Strategic Function in the form of top level capabilities. This will require building new branches onto NATO's existing analytical framework (see Figure 5), which would have the effect of recognizing NATO deterrence functions as a primary competence that is not supported by other cyber capabilities on a secondary basis. Furthermore, the unequal distribution of NATO cyber capabilities along the *Effective C3*, *Effective intelligence*, *Sustainability and Force Protection* strategic capability categories is also apparent already at this level. This demonstrates the value of expanding NATO's set of cyber capabilities along with its theoretical framework to provide equal coverage across all strategic capabilities.

NATO CIS Security Capability Use Case Breakdown Plotted by Function/Capability (Sub-Capability level, excluding Design & Implement)

	Strategic function						
Strategic Capability	Anticipation	Deterrence	Intervention	Normalisation	Prevention	Protection	Stabilisation
Deployability and mobility	16	5	8	12	9	9	13
Effective C3	26	11	16	18	27	22	21
Effective engagement	15	8	13	14	17	15	15
Effective Intelligence	30	18	11	15	37	22	31
Logistics sustainability	19	6	9	13	14	11	17
Survivability and Force Protection	28	18	10	11	27	25	18
Timely Force Availability	14	3	8	12	11	8	13

Figure 18 NATO CIS security second-level capabilities plotted on Strategic Function/Strategic Capability Matrix excluding Design and Implement capability

Figure 18 shows largely the same plotting distribution as Figures 18 and 19. As noted previously, deterrence is covered at a sub-capability level, meaning that NATO cyber capabilities can serve–if not primarily–in some form towards NATO's Deterrence objectives.

Here it is important to note that the unequal distribution of cyber capabilities across Strategic capabilities (*Effective C3*, *Effective intelligence*, *Sustainability and Force Protection*) is not as significant within the Intervention and Normalisation strategic functions. These two functions are important to NATO in particular, as it has no formal, organizational offensive cyber capabilities. However should its operational role within the Cyber domain expand in the future, these strategic functions will have to be better supported by relevant cyber capabilities in order for NATO to pursue its operational or strategic objectives.

As stated before, the existing NATO CIS security capabilities provide coverage across all categories of our analytical framework, however their distribution is not even, and the remain disproportionately allocated to some specific functions and capabilities. Perhaps most strikingly we can observe that existing NATO cyberspace capabilities do not have as much value to the organization's **deterrence** function. At all levels observed and with all filters applied, it remains the strategic function category with the least capability coverage. When filtering for top level capabilities only (see Figure 17: NATO

CIS security top-level capabilities plotted on Strategic Function/Strategic Capability Matrix excluding Design and Implement), it is the only function that has coverage gaps.

Within the deterrence column as displayed, cyberspace capability coverage is on a similar level with other matrix elements for the *Effective command, control and communications*, *Effective intelligence*, and *Survivability and force protection* strategic capabilities. This can be largely explained by NATO's existing CIS capabilities having high facilitatory value and their gearing towards defensive, as opposed to offensive capabilities. When observing the remaining strategic functions that have no coverage, we can determine that they generally have high value for more offensive capabilities, such as *Deployment and mobility*, *Effective engagement*, *Logistics sustainability*, and *Timely force availability*. Because NATO's existing cyber policy recognizes cyber operations as a member state competency, this doesn't pose a serious threat to their current operations, but does weaken the overall effectiveness of its cyber deterrence capabilities on an organizational level.

The capabilities falling under NATO's **normalization** function are also significantly lower than those found in other functions when viewed on a top level. However, this deficiency is less apparent when taking into consideration capabilities at lower levels.

The distribution of capabilities across the strategic capability categories are also important to consider. Here, a higher concentration of use cases can be observed under the following capabilities: *Effective command, control and communications*, *Effective intelligence*, and *Survivability and force protection*. We can attribute this to the current set of NATO use cases being largely built upon existing CIS assets, activities, and processes, which until the classification of Cyber as a domain, held a specific value for facilitating strategic capabilities in other domains (specifically for intelligence and communication capabilities). Emphasis on the protection of existing CIS assets results in the high concentration of capabilities categorized under the Survivability and force protection function.

Overall, the capabilities provide enough coverage to adequately link NATO's strategic capabilities with its strategic functions, however there remains some degree of development needed to fully develop its cyberspace capabilities to account for the new, broader scope of its possible activities in cyberspace. Our analytical framework provides a prioritization mechanism that can assist in quantifying the costs and importance of different capabilities and capacities at all levels and provides an effective tool to improve NATO cyberspace capabilities.

4 Conclusions and Recommendations

4.1 Conclusions

Based on our review of literature, analysis of the existing NCIA analytical framework, and refining as well as tailoring the HCSS in-house framework to fit the one used by NCIA , we have reached the following conclusions.

1. Current cyber capability requirements and approaches do no take the full scope and depth of Cyber as a Domain in consideration. Future focus by NATO Strategic Commands could be considerably broadened. The scope and depth of NATO's current cyber capability framework should reflect this broader scope.
2. Possible broadening of the current cyberspace analytical framework can be found in emphasizing its deterrence and intervention capabilities and strengthening the notion that as a result of considering Cyber as a Domain it contains operational capabilities in their own right.
3. The alignment of thinking and clarity of roles and responsibilities between the NATO Strategic Commands and the Member States, and between the different domains need further attention.
4. There are options to further strengthen NATO cyber capabilities by involving more Non-state actors.
5. The proposed extended framework could create more awareness, thus deepening and operationalizing capability development.

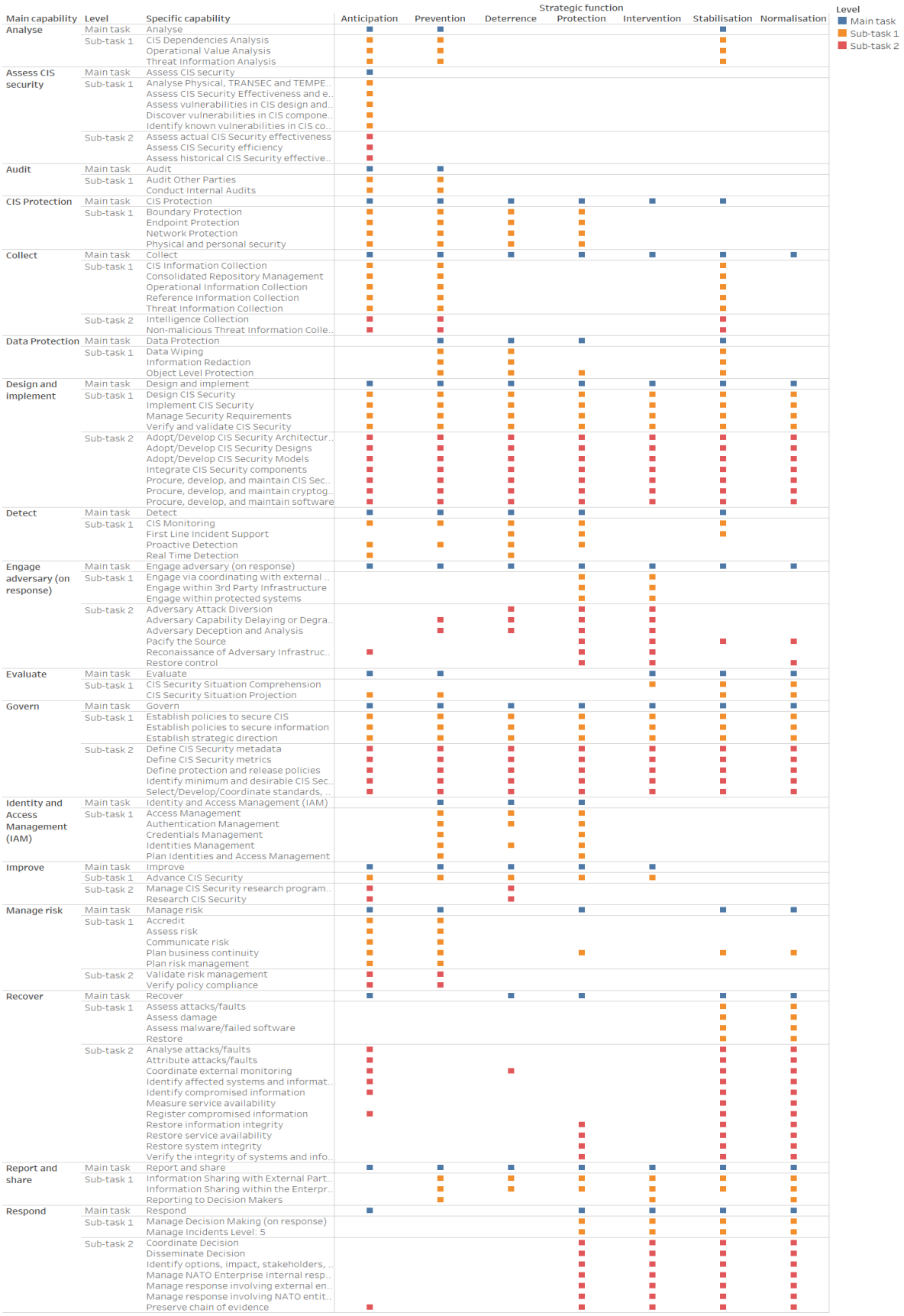
4.2 Recommendations

1. It is recommended that the concept of Cyber as a Domain needs more operational attention regarding the development of capabilities for strategic functions which at the moment are underdeveloped, such as deterrence and intervention.
    a. For the strategic function deterrence some example the following use cases could be illustrative:
        i. Operational Readiness Posture (#7)
        ii. Resilient Cyber C3 Posture (#14)
        iii. All-Source Attack Attribution (#21)
        iv. Cyber Strategic Communications (#28)
        v. Non-National, Non-Military Response (#35)
        vi. Enemy Cyberstrike Response Posture (#42)
        vii. Concerted Deterrence Strategies (#49)
    b. For the strategic function intervention some example the following use cases could be illustrative:
        i. Cyber Deception (#5)
        ii. Whole of Gov Cyber Response (#12)
        iii. Assessment of Vulnerability of Potential Cyber Targets (#19)
        iv. Cyber Escalation Control (#26)
        v. Integrated Operational Cyber Readiness (#33)
        vi. Protection of Cyber Assets (#40)
        vii. OCEO Infrastructure (#47)
    c. For capabilities that enhance Non-state actor involvement:
        i. Whole-of-Nation Defense (#6)

ii. Cyber Non-NATO Cooperation Capability (#11)
iii. Integrated Cyber Situational Understanding (#18)

2. To further develop the understanding and awareness of the concept of cyber as a domain it is to be considered that activities are deployed to enhance the thinking on the concept, familiarize the different levels of the Strategic Commands and utilize the possibility to organize extra input of ideas and suggestions for NATO to further enhance its cyber capabilities, both for the NATO Strategic Commands and as well as the Member States.

5 Appendix 1. Full visuals



Main capability	Level	Specific capability
Analyse	Main task	Analyse
	Sub-task 1	CIS Dependencies Analysis
		Operational Value Analysis
		Threat Information Analysis
Assess CIS security	Main task	Assess CIS security
	Sub-task 1	Analyse Physical, TRANSEC and TEMPE..
		Assess CIS Security Effectiveness and e..
		Assess vulnerabilities in CIS design and..
		Discover vulnerabilities in CIS compone..
		Identify known vulnerabilities in CIS co..
	Sub-task 2	Assess actual CIS Security effectiveness
		Assess CIS Security efficiency
		Assess historical CIS Security effective..
Audit	Main task	Audit
	Sub-task 1	Audit Other Parties
		Conduct Internal Audits
CIS Protection	Main task	CIS Protection
	Sub-task 1	Boundary Protection
		Endpoint Protection
		Network Protection
		Physical and personal security
Collect	Main task	Collect
	Sub-task 1	CIS Information Collection
		Consolidated Repository Management
		Operational Information Collection
		Reference Information Collection
		Threat Information Collection
	Sub-task 2	Intelligence Collection
		Non-malicious Threat Information Colle..
Data Protection	Main task	Data Protection
	Sub-task 1	Data Wiping
		Information Redaction
		Object Level Protection
Design and implement	Main task	Design and implement
	Sub-task 1	Design CIS Security
		Implement CIS Security
		Manage Security Requirements
		Verify and validate CIS Security
	Sub-task 2	Adopt/Develop CIS Security Architectur..
		Adopt/Develop CIS Security Designs
		Adopt/Develop CIS Security Models
		Integrate CIS Security components
		Procure, develop, and maintain CIS Sec..
		Procure, develop, and maintain cryptog..
		Procure, develop, and maintain software
Detect	Main task	Detect
	Sub-task 1	CIS Monitoring
		First Line Incident Support
		Proactive Detection
		Real Time Detection
Engage adversary (on response)	Main task	Engage adversary (on response)
	Sub-task 1	Engage via coordinating with external ..
		Engage within 3rd Party Infrastructure
		Engage within protected systems
	Sub-task 2	Adversary Attack Diversion
		Adversary Capability Delaying or Degra..
		Adversary Deception and Analysis
		Pacify the Source
		Reconaissance of Adversary Infrastruc..
		Restore control
Evaluate	Main task	Evaluate
	Sub-task 1	CIS Security Situation Comprehension
		CIS Security Situation Projection
Govern	Main task	Govern
	Sub-task 1	Establish policies to secure CIS
		Establish policies to secure information
		Establish strategic direction
	Sub-task 2	Define CIS Security metadata
		Define CIS Security metrics
		Define protection and release policies
		Identify minimum and desirable CIS Sec..
		Select/Develop/Coordinate standards, ..
Identity and Access Management (IAM)	Main task	Identity and Access Management (IAM)
	Sub-task 1	Access Management
		Authentication Management
		Credentials Management
		Identities Management
		Plan Identities and Access Management
Improve	Main task	Improve
	Sub-task 1	Advance CIS Security
	Sub-task 2	Manage CIS Security research program..
		Research CIS Security
Manage risk	Main task	Manage risk
	Sub-task 1	Accredit
		Assess risk
		Communicate risk
		Plan business continuity
		Plan risk management
	Sub-task 2	Validate risk management
		Verify policy compliance
Recover	Main task	Recover
	Sub-task 1	Assess attacks/faults
		Assess damage
		Assess malware/failed software
		Restore
	Sub-task 2	Analyse attacks/faults
		Attribute attacks/faults
		Coordinate external monitoring
		Identify affected systems and informat..
		Identify compromised information
		Measure service availability
		Register compromised information
		Restore information integrity
		Restore service availability
		Restore system integrity
		Verify the integrity of systems and info..
Report and share	Main task	Report and share
	Sub-task 1	Information Sharing with External Part..
		Information Sharing within the Enterpr..
		Reporting to Decision Makers
Respond	Main task	Respond
	Sub-task 1	Manage Decision Making (on response)
		Manage Incidents Level: 5
	Sub-task 2	Coordinate Decision
		Disseminate Decision
		Identify options, impact, stakeholders, ..
		Manage NATO Enterprise Internal resp..
		Manage response involving external en..
		Manage response involving NATO entit..
		Preserve chain of evidence

Figure 19 Specific capabilities by strategic function

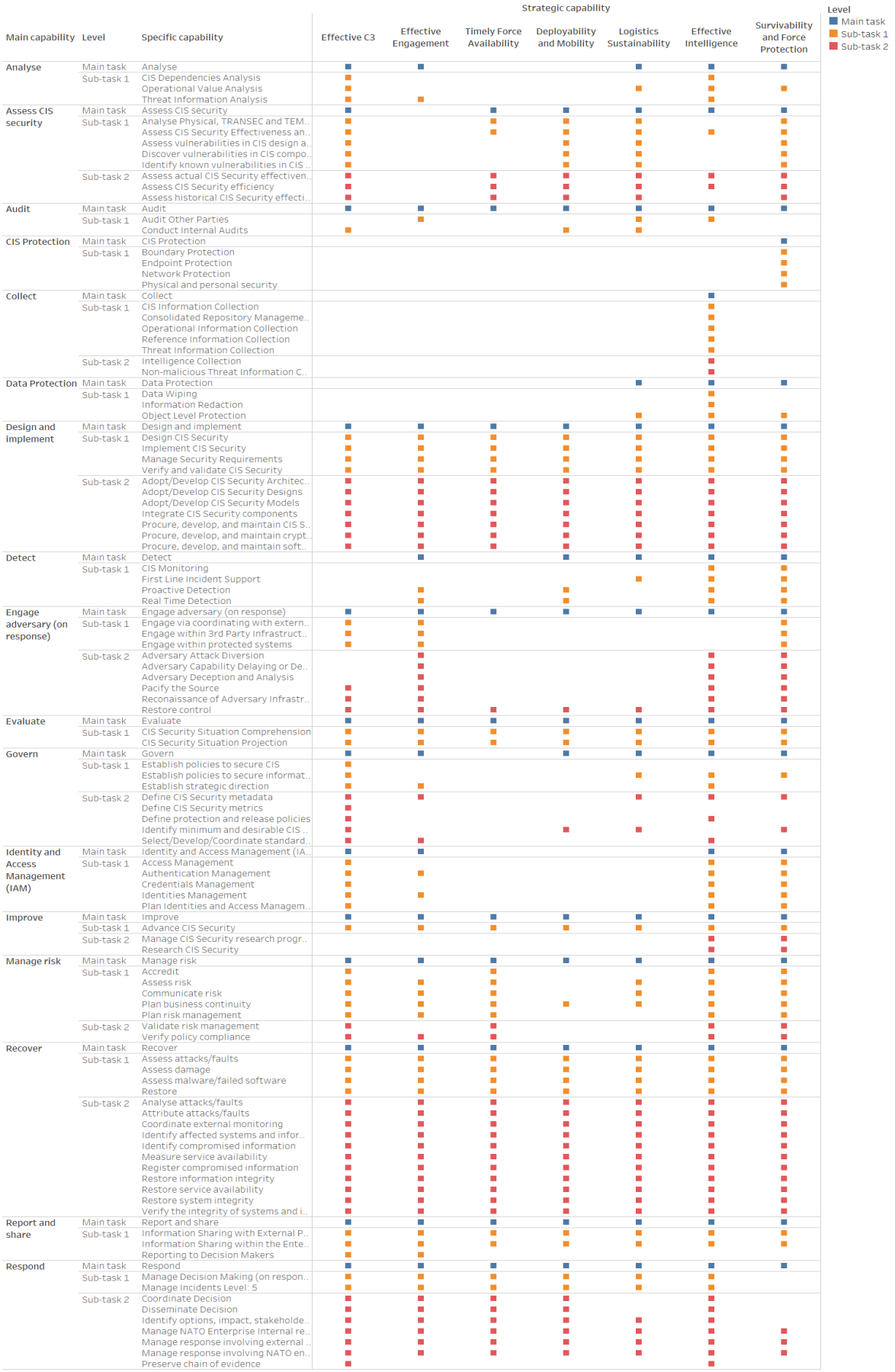


Figure 20 Specific capabilities by strategic capabilities

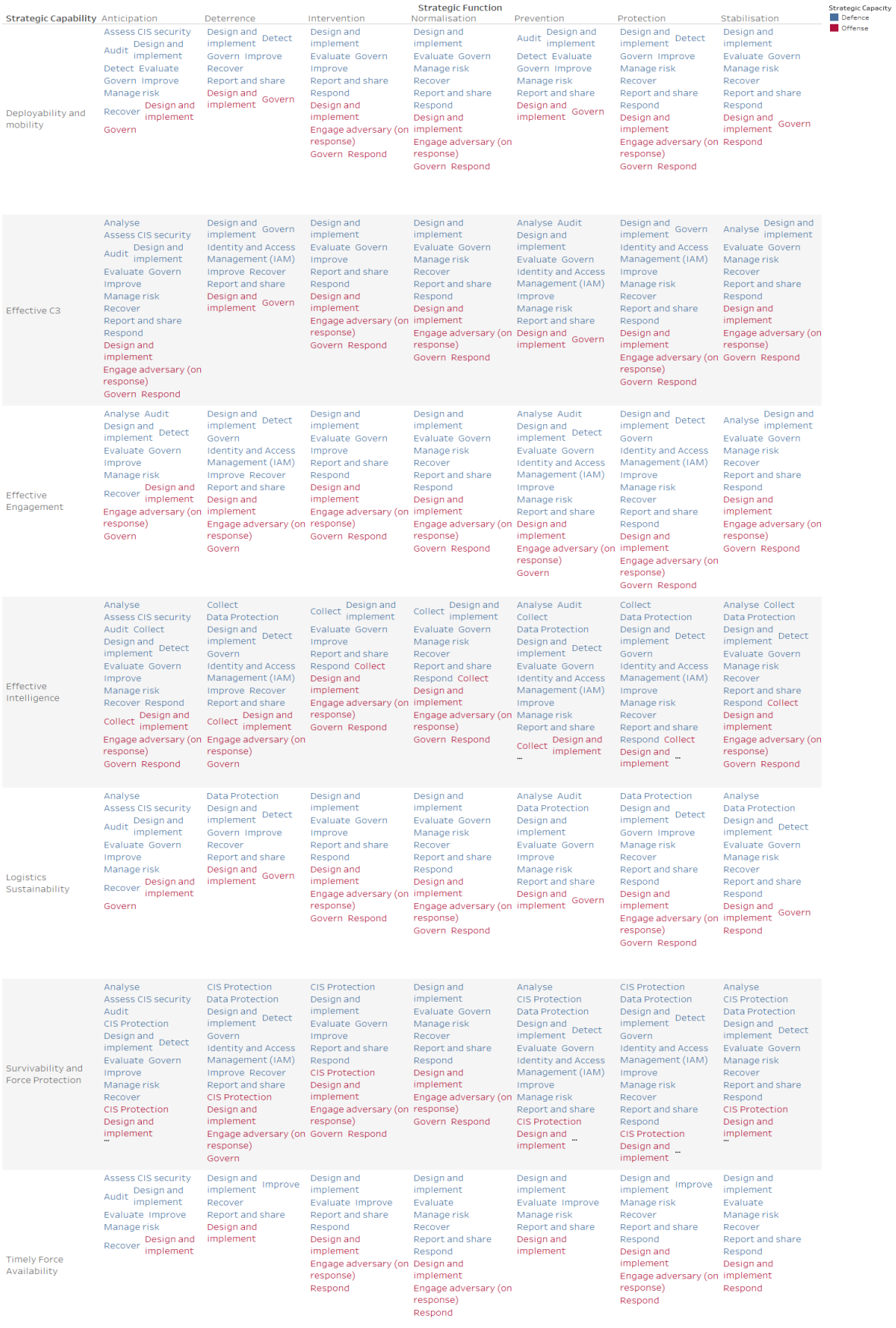


Figure 21 Structure by defence/offense

Figure 22 Structure by non-state partnerships

6 Appendix 2. HCSS set of example use cases

The HCSS set of example use cases were developed as a result of an earlier research effort commissioned by the Netherlands Ministry of Defence. For our board game these were represented by a physical set of cards, each displaying information on a distinctive test case that could then be positioned within the matrix.

The use case cards consist of different elements, such as a clear title that addresses precisely what the capability is about, a definition following a consistent syntax ("*The ability to* … [do something] … [with an intended effect and or outcome]"), and scoring elements that can assist in assessing a use case's importance and cost.

The physical cards and their designs are developed by HCSS and were transformed into a full game, for which HCSS possesses a copyright.

Figure 23 HCSS Empty capability card example

1 FORWARD LOOKING TRAINING

THE ABILITY TO CONDUCT "FUTURE-PROOF" TRAINING IN SPITE OF RAPID CHANGES IN TECHNOLOGY

EXAMPLES
- FBI National Cyber-Forensics & Training Alliance
- ISO 2700X programs

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐
Maturity 0, 1, 2, 3	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs	☐	☐	☐
Change Processes	☐	☐	☐

2 ANTICIPATIVE ADVERSARY INTENT IN R&D

THE ABILITY TO INVEST IN R&D TO ANTICIPATE ADVERSARIES INTENT FOR MINIMUM OF 2 TO 3 YEARS

EXAMPLES
- Cyber Threat Analysis
- US IARPA

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐
Maturity 0, 1, 2, 3	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs	☐	☐	☐
Change Processes	☐	☐	☐

3 INADVERTENT ESCALATION AVOIDANCE

THE ABILITY TO REDUCE THE RISK OF MISUNDERSTANDING OF CYBER OFFENSIVE TRIGGERS BETWEEN COMPETING PARTIES BY ENGAGING IN NORMS AND CBMS DISCUSSIONS

EXAMPLES
- Cyber Threat Analysis
- Diplomat CBM activity (UNGGE/norms, OSCE, bilats)

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐
Maturity 0, 1, 2, 3	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs	☐	☐	☐
Change Processes	☐	☐	☐

4 CYBER SECURITY CAPACITY BUILDING

THE ABILITY TO INCREASE OVERALL CYBER SECURITY GLOBALLY AND DECREASE BAD INFRASTRUCTURE AND ATTACK SURFACE

EXAMPLES
- GFCE, Mil-Mil Programs
- EEAS Programs

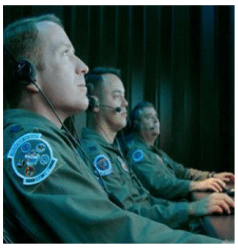
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐
Maturity 0, 1, 2, 3	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs	☐	☐	☐
Change Processes	☐	☐	☐

5 CYBER DECEPTION

THE ABILITY TO MASK INTENTIONS IN CYBERSPACE AND CONCEAL OPERATIONS AND ASSETS



EXAMPLES
- JP 3-13 MILDEC Strategy

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

6 WHOLE-OF-NATION DEFENSE

THE ABILITY TO COOPERATE LONG-TERM WITH LAW ENFORCEMENT INSTITUTIONS, PRIVATE SECTOR AND CI PROVIDERS TO EXCHANGE EXPERTISE AND INFORMATION

EXAMPLES
- Information Sharing and Analysis Centers, Trusted Network initiative
- National Cybersecurity and Communications Integration Center

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

7 OPERATIONAL READINESS POSTURE

THE ABILITY TO PREPARE OFFENSIVE AND DEFENSIVE FORCES TO SHOW READINESS TO ADVERSARIES IN ORDER TO DETER THEM FROM USING OWN INSTRUMENTS

EXAMPLES
- International Cyber Readiness Assessment Framework
- Strategic Communications Strat.

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

8 MULTILEVEL RISK ASSESSMENT MONITORING

THE ABILITY TO ESTIMATE VARIOUS LEVELS OF DANGER FROM CYBERSPACE TO IMPLEMENT ADEQUATE PROTECTION MEASURES

EXAMPLES
- Information Operations Conditions
- Model Driven Risk Analysis

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

9 ENHANCED SITUATIONAL AWARENESS

THE ABILITY TO PROVIDE TIMELY CRITICAL INFORMATION TO OPERATIONAL AND STRATEGIC DECISION MAKING AND INFORM SITUATONAL AWARENESS

EXAMPLES
- GCHQ - CSOC
- US DoD/DHS – ESSA imitative

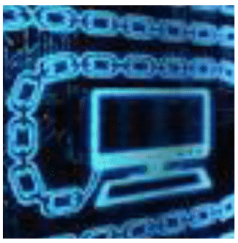
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

10 CYBER SECURITY CHAIN RESILIENCE

THE ABILITY TO SYNCHRONISE SECURE CYBER CHAIN RESILIENCE TO PREVENT ADVERSARIES FROM INTERVENING



EXAMPLES
- Defense Procurement Regulations
- Export Restrictions

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

11 CYBER NON-NATO COOPERATION CAPABILITY

THE ABILITY TO PREPARE FLEXIBLE DIPLOMATIC AND C3 STRUCTURES CAPABLE OF ENGAGING IN CYBER DIALOGUE WITH NON-NATO NATIONS

EXAMPLES
- NATO MNE-5
- Joint Force Headquarters-Cyber

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

12 WHOLE-OF-GOV CYBER RESPONSE

THE ABILITY TO STRENGTHEN THE LINKS BETWEEN MILITARY AND CIVILIAN COMMAND TO PROVIDE REAL TIME ANALYSIS AND RESPONSE

EXAMPLES
- Memorandum of agreement between DHS and DoD
- NL National Detection Network

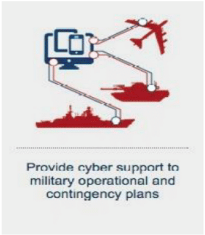
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

13 EXPEDITIONARY CYBER ADVISORY TEAM

THE ABILITY TO DEPLOY EXPEDITIONARY ADVISORY CAPACITY TEAMS TO DEPLOYED FORCES IN THE FIELD



EXAMPLES
- US Combat Mission Teams
- Defence Cyber Operations Group

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

14 RESILIENT CYBER C3 POSTURE

THE ABILITY TO BUILD RESILIENT C3 STRUCTURES THAT CAN WITHSTAND ATTEMPTS OF DISRUPTION

EXAMPLES
- Resilient and Redundant Systems
- Cyber Resiliency Engineering System

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

15 ALLIED CYBER SECURITY CAPACITY

THE ABILITY TO BUILD POLICY AND TECHNICAL CYBER DEFENSE CAPABILITIES AMONG ALLIES.

CCDCOE
Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia

EXAMPLES
- NATO Cooperative Cyber Defence Centre of Excellence
- NATO RRT

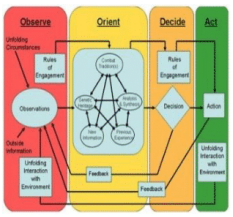
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

16 MULTILEVEL CYBER ADVERSARY THREAT ASSESSMENT

THE ABILITY TO CONDUCT MULTILEVEL, INTEGRATED AND COMPREHENSIVE THREAT ASSESMENT ON ADVERSARIES CAPABILITIES AND INTENT



EXAMPLES
- UK C-SOC
- US CTIIC

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

17 CYBER COUNTER INTELLIGENCE CAPABILITY

THE ABILITY TO STRENGTHEN INTERNAL MONITORING TO DETECT AND PREVENT INSIDER THREATS

EXAMPLES
- Implementing least privilege access
- Controlling sensitive data

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

18 INTEGRATED CYBER SITUATIONAL UNDERSTANDING

THE ABILITY TO USE ALL SOURCE AND NON-NATO CYBER INTELLIGENCE CAPABILITIES TO PROVIDE FULL OPERATIONAL UNDERSTANDING

EXAMPLES
- Private Companies Analysis
- Treemap of Open Sources Reporting Cyber Attacks

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

19 ASSESSMENT OF VULNERABILITY OF POTENTIAL CYBER TARGETS

THE ABILITY TO DELIVER PERSISTENT AND ACCURATE TARGET INTELLIGENCE, PROCESS AND EXPLOIT OF COLLECTED CYBER VULNERABILITY DATA

EXAMPLES
- CS-East's Cyber Defense and Intelligence
- CNE Operations

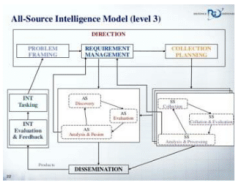
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

20 CYBER INTELLIGENCE CAPABILITY BUILDING

THE ABILITY TO BUILD MILITARY AND CIVILIAN INTELLIGENCE TO EVALUATE AND FEEDBACK INTELLIGENCE EFFECTIVENESS AND QUALITY



EXAMPLES
- Cyber Intelligence Tradecraft Project
- Cyber Intelligence Task Force

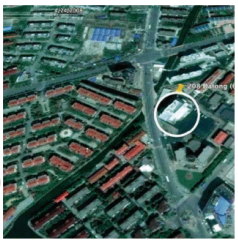
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

21 ALL-SOURCE ATTACK ATTRIBUTION

THE ABILITY TO ATTRIBUTE WITH MEDIUM-HIGH CONFIDENCE CYBER ACTORS, USING A COMBINATION OF MEANS IN A STRUCTURED METHODOLOGY



EXAMPLES
- Industry reports (MANDIANT etc.)
- SIGINT, HUMINIT, CYINT

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

22 CYBER TECHNOLOGY FORESIGHT ANALYSIS

THE ABILITY TO ESTABLISH CYBER TECHNOLOGY FORESIGHT ANALYSIS TO PREPARE TIMELY THREAT MITIGATION MEASURES

EXAMPLES
- Institute for Technology Assessment
- The Strategic Foresight Initiative

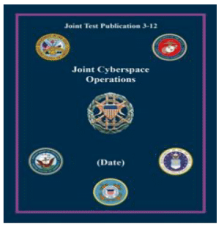
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

23 STRATEGIC CYBER PLANNING ARCHITECTURE

THE ABILITY TO TIE STRATEGIC CYBER PLANNING FRAMEWORKS WITH INTELLIGENCE AND HORIZON SCANNING TO PRIORITIZE TARGETS AND THE APPROPRIATE RESPONSE



EXAMPLES
- The Joint Force Commander's Guide to Cyberspace
- PDD -20

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

24 UNDERSTANDING CONSEQUENCES OF CYBER CONFLICT

THE ABILITY TO DRIVE DISCUSSION ON MEANS OF WAGING AND CONTROLLING CYBER CONFLICTS THROUGH PUBLICLY CONDUCTED RESEARCH

EXAMPLES
- US Defense Science Board publications
- Dutch Cyber Security Council

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

25 CYBER ROE FRAMEWORK

THE ABILITY TO ESTABLISH ROES WITHIN THEATER TO COORDINATE EFFECTIVE PROPORTIONATE ENGAGEMENT

EXAMPLES
- Tallinn Manual
- UN GGE report

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

26 CYBER ESCALATION CONTROL

THE ABILITY TO DETERMINE AND CONTROL ENGAGEMENT ESCALATION

EXAMPLES
- The C-J-K Cyber Hotline
- Shared Threat Assessments

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

27 INTERNATIONAL STANDARDS

THE ABILITY TO DEVELOP INTERNATIONAL STANDARDS AND PRACTICES TO RAISE OVERALL IA AWARENESS

EXAMPLES
- Internet Engineering Task Force
- National Institute of Standards and Technology

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

28 CYBER STRATEGIC COMMUNICATIONS

THE ABILITY TO COMMUNICATE STRATEGIC INTENT AND CAPABILITIES TO DETER ADVERSARIES

EXAMPLES
- Cyber strategies
- Targeted leaks and messaging

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

29 INTER-ENTERPRISE IPS DEPLOYMENT

THE ABILITY TO DEPLOY AN ENTERPRISE-WIDE INTRUSION PROTECTION SYSTEMS ACROSS PARNTERS WITH STABLE INDICATORS OF COMPROMISE

EXAMPLES
- Einstein 3A System, DECS
- Netherlands Detection Network

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

30 MILITARY-SUPPORTED VULNERABILITY DISCLOSURE

THE MILITARY ABILITY TO DELIVER TO THE PUBLIC NEWLY DISCOVERED ZERO DAYS AS PART OF NATIONAL PUBLIC RESPONSIBLE DISCLOSURE POLICY

EXAMPLES
- Exploiting Zero-Days

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

31 FORWARD CYBER DEFENSE

THE ABILITY TO SEND CYBER MILITARY ADVISORY TEAMS TO STRENGTHEN PREVENTION CAPABILITIES

US-CERT
United States Computer Emergency Readiness Team

EXAMPLES
- CERT Advisory Team
- FBI Cyber Action Team

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

32 INTEGRATED CYBER SUPPORT

THE ABILITY TO DEPLOY SUPPORT TEAMS FOR MISSION FORCE COMMANDER TO INCREASE STABILIZING EFFORTS

EXAMPLES
- US Special Collection Service
- NSA CLA

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

33 INTEGRATED OPERATIONAL CYBER READINESS

THE ABILITY TO SYSTEMATICALLY MAINTAIN HIGH READINESS INTEGRATED FORCES READY TO INTERVENE

EXAMPLES
- National Cyber Awareness System
- Cyber Response Forces

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

34 CYBER POLICY ADVISORY

THE ABILITY TO ADVISE SENIOR LEADERSHIP AND LAWMAKERS ON ASPECTS OF CYBER OPERATIONS

EXAMPLES
- US NSA legislative affairs
- National Security Council

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

35 NON-NATIONAL, NON- MILITARY RESPONSE

THE ABILITY TO EMPHASIZE NON-MILITARY AND NON-NATIONAL CAPABILITIES DEPLOYMENT TO RESPOND ADVERSARIES

EXAMPLES
- Private Sector Cyber Teams
- The Europol Cyber Intelligence Team

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

36 CYBER DATAFLOW MANEUVER CONTROL

THE ABILITY TO ESTABLISH HIGHLY SECURE WORK ZONES AND FREE MANEUVER OF DATA

EXAMPLES
- Highly Secure Wi-Fi in Military Bases Abroad
- Battlefield Anti-Intrusion System

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

37 ADAPTIVE CYBER SECURITY DEFENSE

THE ABILITY TO COMPILE STRONG CYBER SECURITY TOOLBOX TO ANTICIPATE CHALLENGES FOR FORCE AND WEAPONS SURVIVABILITY

EXAMPLES
- Network Security Analysis Toolbox
- Network Security Toolkit

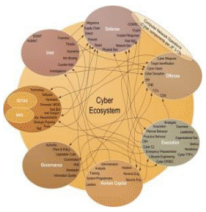
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

38 MILITARY CAPACITY ECO-SYSTEM CONTRIBUTION

THE ABILITY TO CONTRIBUTE WITH MILITARY CAPACITIES TO SECURE CYBERSPACE ECOSYSTEM



EXAMPLES
- Smart Grid System
- Maturity Model for Networked Environments

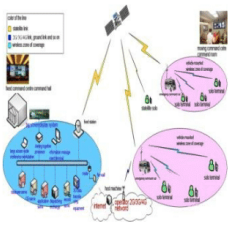
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

39 PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURE

THE ABILITY TO PHYSICALLY PROTECT EMERGENCY COMMUNICATION FACILITIES TO INCREASE STABILISATION EFFORTS



EXAMPLES
- United States Nuclear Regulatory Commission
- Emergency communications

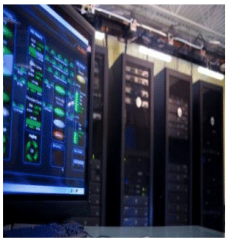
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

40 PROTECTION OF CYBER ASSETS

THE ABILITY TO PROTECT ALL CYBER ASSETS FROM PHYSICAL THREATS



EXAMPLES
- DHS Coordinated Approach
- Strategy for the Physical Protection of Critical

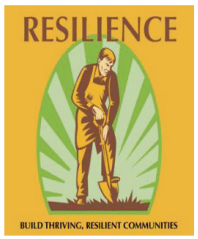
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

41 RESILIENT SYSTEM RESTORATION

THE ABILITY TO BUILD RESILIENT SYSTEMS TO QUICKLY RESTORE NORMAL CONDITIONS AFTER AN ATTACK



EXAMPLES
- Data Center Resiliency
- Engineered Resilient Systems

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

42 ENEMY CYBERSTRIKE RESPONSE POSTURE

THE ABILITY TO SURVIVE ENEMY CYBERSTRIKE AND RESPONSE WITH COUNTER ATTACK TO DETER THE ADVERSARIES

EXAMPLES
- Nuclear Second Strike
- Attributing Attack

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

43 MULTILEVEL THREAT COMPOSITION

THE ABILITY TO COMPOSE MULTILEVEL THREAT PICTURE TO PROTECT FORCE SURVIVABILITY

EXAMPLES
- Cyber Risk Matrix
- Cyber Threat Source Descriptions

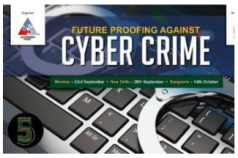
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

44 FUTURE-PROOF TECHNOLOGY TESTING

THE ABILITY TO PERFORM FUTURE-PROOF TECHNOLOGY TESTING TO ANTICIPATE ADVERSARIES THREAT TO LOGISTICS



EXAMPLES
- Data-Collection Methods
- National testbeds (sandbox) or Cyberranges

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?	☐	☐	☐
Can it be used independently?	☐	☐	☐
Can it be integrated easily?	☐	☐	☐

	LOW	MEDIUM	HIGH
Training of Personnel	☐	☐	☐
Costs of Procurement	☐	☐	☐
Change Processes	☐	☐	☐

45 DEFENCE ACADEMY CYBER CONFLICT PREVENTION

THE ABILITY TO SET UP TRAINING AND EDUCATION ON CYBER CONFLICT PREVENTION

EXAMPLES
- Norwegian Cyber Defence Academy
- Georgia Cyber Academy

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

46 AD HOC MILITARY WIDE AREA NETWORK

THE ABILITY TO EXTEND MILITARY WIDE-AREA-NETWORKS TO ESTABLISH COMMUNICATION ACROSS MISSION AREAS

EXAMPLES
- Army's World-Wide Satellite Systems
- Internet in Suitcase

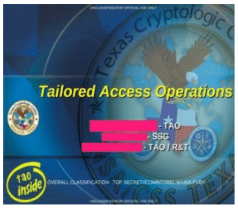
REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

47 OCEO INFRASTRUCTURE

THE ABILITY TO BUILD OCEO INFRASTRUCTURE TO STRENGTHEN INTERVENTION CAPABILITIES



EXAMPLES
- TAO Unit in NSA
- 67th Cyberspace Operations Wing

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

48 HOST NATION CYBER LOGISTICS CAPABILITY BUILDING

THE ABILITY TO PROVIDE TEMPORARY ASSISTANCE TO PROTECT HOST NATION "CI" (E.G. AIRPORTS, PORTS)

EXAMPLES
- Cybersecurity Monitoring and Logging Guide
- Center of Cyber Logistics

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

49 CONCERTED DETERRENCE STRATEGIES

THE ABILITY TO DELIVER AND MAINTAIN CONCERTED DETERRENCE STRATEGIES TO INFORM ADVERSARIES ON OUR RESPONSE CAPABILITIES

EXAMPLES

- Deterrence Doctrines
- Deterrence by Denial

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			

50 CYBER SECURE SUPPLY CHAIN

THE ABILITY TO SECURE SUPPLY CHAIN TO PROTECT LOGISTICS

EXAMPLES

- Banning Software from Certain Countries
- CIS Critical Security Controls

REASONS TO NEED THIS CAPABILITY

	LOW	MEDIUM	HIGH
How strategically important is it?			
Can it be used independently?			
Can it be integrated easily?			

	LOW	MEDIUM	HIGH
Training of Personnel			
Costs of Procurement			
Change Processes			