2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis

Max Smeets
Center for International Security and Cooperation
Stanford University
Stanford, United States
MwSmeets@stanford.edu

Abstract: NATO member states are starting to talk more openly about the incentives and opportunities to conduct offensive cyber operations for military purposes. This growing interest in 'offensive cyber' is most clearly expressed in the creation of cyber commands, branches or services within the armed forces. Little research, however, has analyzed these organizational developments. This article provides a conceptual framework to facilitate empirical analysis across military cyber organizations (MCOs). The framework distinguishes between five stages of organizational development: i) seed, ii) startup, iii) growth, iv) expansion, and v) maturity. Our empirical analysis reveals that a significant number of NATO members started to carefully consider establishing MCOs from 2008 onwards, and some states had already started significant organizational efforts in the 1990s. However, I also reveal that the MCOs of most NATO members are still at the early stages of organizational development, and even those at the growth stage still have limited budgets to address the different workforce, capability, strategic and other requirements.

Keywords: *NATO, military cyber organization, offensive cyber operations, development life cycle*

1. INTRODUCTION

Over the years, NATO members have presented and rolled out several plans for improving cyber-defense governance. Official commitments made at NATO summits on cyber security have become increasingly granular.[1] One topic that government leaders have long avoided talking about, however, is their *own* willingness and capacity to conduct military cyber operations.

Times are changing. As one senior official put it at a military cyber conference: "Speaking at NATO about offensive cyber was blasphemy a few years ago. We have advanced".[2] Last year the Alliance reached a landmark that went largely unnoticed: there are now more member states which have publicly declared they are seeking to establish an offensive cyber capability than there are member states which have remained publicly silent on this issue.[3] In late 2018, it was also announced that five countries would contribute national cyber forces to NATO missions and operations. This group consists of the United States, the United Kingdom, Denmark, Estonia, and the Netherlands.[4]

The growing interest in offensive cyber operations for military purposes is most clearly expressed in the creation of cyber commands, branches or services within the armed forces. These military cyber organizations (MCOs), as Piret Pernik from ICDS noticed in her study, are often predicated "by the need to centralise, consolidate, and streamline formerly fragmented capabilities and organisations, while eliminating overlapping roles and responsibilities" to effectively operate in this new "operational domain".[5]

Academic scholarship and policy research is still lagging behind in analyzing these developments. We still lack a comprehensive overview of where NATO member

[1] These include: Prague (2002), Riga (2006), Bucharest (2008), Strasbourg (2009), Lisbon (2010), Chicago (2012), Wales (2014), Warsaw (2016) and Brussels (2018). For a good overview on early thinking see: John B. Sheldon, "NATO and Cyber Defense: Hanging Together or Hanging Separately?", Presentation, (year unknown), hxxp://www.unidir.ch/files/conferences/pdfs/nato-and-cyber-defence-hanging-together-or-hanging-separatelyen-1-608.pdf.

[2] See: Dutch Ministry of Defense, Third International Cyber Operations Symposium, (2017, October); also see: Sophie Arts, "Offense as the New Defense: New Life for NATO's Cyber Policy," The German Marshall Fund of the United States, Policy Brief, 39, (2018):1-9.

[3] 'Offensive cyber capability' refers in this context to a broad set of capabilities referred to by states, including 'cyberwarfare capabilities'. 'military cyber arsenal', 'Computer Network Attack capabilities', and 'military cyber offense'. Section IV provides a more detailed overview on the use of different terminology and developments within each country.

[4] US Department of Defense, "News Conference By Secretary Mattis at NATO Headquarters, Brussels, Belgium," US Department of DEcen, (2018, October 4), retrieved from: dod.defense.gov; Also see the Brussel Summit Declaration for a reaffirmation of NATO mandate and cyber efforts: NATO, "Brussels Summit Declaration, (2018, July 11-12), retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-summit-declaration-eng.pdf.

[5] Piret Pernik, "Preparing for Cyber Conflict: Case Studies of Cyber Command," (2018, December), retrieved from: https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf.

states stand in terms of organizational development. The purpose of this article is therefore to provide a conceptual framework to facilitate analysis and comparison between different MCOs.[6]

This paper's argument is developed in five parts. Section II provides a framework which distinguishes between five stages of organizational development: i) seed and development, ii) startup, iii) growth, iv) expansion, and v) maturity. Section III offers an empirical perspective, providing an historical overview of member states' organizational achievements. The section indicates that a significant number of NATO members started to think about military cyber operations from 2008 onwards, and some states had already started significant organizational efforts in the 1990s. Yet, I also reveal that the MCOs of most states are still at the early stages of organizational development, and even those at the growth stage still have limited budgets. Section IV provides additional considerations about NATO members' MCO development. Section V concludes and identifies avenues for future research.

2. A CONCEPTUAL FRAMEWORK FOR MCOS

A military cyber organization is defined as a command, service, branch or unit within a government's armed forces which has the authority and mission to conduct offensive cyber operations to disrupt, deny, degrade and/or destroy (d4 effects).

MCOs come in all shapes and forms. Countries have different strategic objectives and approaches and base their decisions on different legal and organizational prerequisites. In some countries, MCOs can be authorized to direct and control the full spectrum of cyber operations. Other MCOs only have the narrow authority (following a mandate) to execute a small set of offensive missions. Some states' MCOs are small: their workforce could easily fit into a few school buses; for others, you would need a fleet of Boeing 747s to transport its workforce. Finally, some MCOs are expected to play a role in defense and resiliency efforts such as assisting civilian authorities in protecting critical infrastructure. Others are not.

Given this variation in MCOs, we must use a framework that balances two considerations: on the one hand, the framework needs to be sufficiently general to incorporate significant variation in missions and organizational structures; whilst, on the other hand, the framework's categorical distinctions need to be specific enough to capture empirical progress in a meaningful manner.

In finance and business management literature, the concept of the 'business life cycle'

[6] The goal of this article is not to provide an in-depth case study of a specific country's organizational development. Nor is the purpose of this research to explain why states seek to establish MCOs. For an analysis of this question see: Max Smeets, "Going cyber : the dynamics of cyber proliferation and international security," DPhil Dissertation in International Relations, University of Oxford, 2017.

is widely used to help with the strategic planning and operations of a company.[7] The idea is that the progression of a company can be divided into several stages, each with its own opportunities and challenges. For example, a small business will initially have to focus on market acceptance and determining a profitable business structure. It subsequently needs to think more carefully about how it can establish a customer base and manage financial issues such as funding and cash reserves. In later stages, different issues will have to be considered, such as dealing with (increased) market competition and expanding into new markets and distribution channels. Solutions which may have worked for one stage may not work in another. This means that businesses have to adjust operations accordingly.[8]

MCOs are not corporations, yet we can deploy a similar framework for this type of institutional development.[9] An overview of the stages and their associated challenges is provided in *Table I: The Life Cycle of an MCO*.

TABLE I: THE LIFE CYCLE OF AN MCO

Stage	Description
Seed & Development	A government recognizes the importance of investing in offensive cyber, and talks about the need to establish an MCO.
Startup / Launch	There is the political authorization to establish an MCO
Growth	The MCO has moved towards an actual operational capacity.
Expansion	The MCO has repeatedly conducted offensive cyber operations and is potentially assessing new options for further development.
Maturity	The MCO is able to conduct full spectrum operations against a wide range of targets, embedded in a strategy that has proven to be effective.

Each NATO member state begins at the *seed and development* phase: this is when senior officials within the government start to discuss the importance of establishing an MCO to conduct offensive cyber operations.[10] A government moves to the *startup* phase when the political authorization to establish an MCO is issued.[11] During the

[7] Neil Petch, "The Five Stages Of Your Business Lifecycle: Which Phase Are You In?," *Entrepreneur*, (2016, February 29), retrieved from: https://www.entrepreneur.com/article/271290 For an alternative overview see: Neil C. Churchill and Virginia L. Lewis, "The Five Stages of Small Business Growth," *Harvard Business Review*, (1983, May), retrieved from: https://hbr.org/1983/05/the-five-stages-of-small-business-growth.

[8] In the same vein, unresolved challenges from an earlier stage may also come to haunt a business at later stages. For example, missing a lack of accounting management initially might hinder to have an accurate reflection of the later business finances.

[9] Whilst using the same categories, I do not mean to suggest that the dynamics underlying each stage of organizational development are the same for MCOs as a business.

[10] This generally accumulates into a national security strategy which indicates that the government should start to invest in 'offensive cyber capabilities'. There could be multiple reasons why the governments starts to talk about the need to establish an MCO – one could be the strategic landscape.

[11] Political authorization may come from various authorities, such as the parliament, government, president or minister of defense. It is normally part of the defense planning.

growth stage the MCO begins developing an actual operational capability. When an MCO has started to conduct offensive cyber operations it enters the *expansion* phase. The final stage of the MCO life cycle is called *maturity*: an MCO at this stage is able to conduct full spectrum operations against a wide range of targets, as part of a deliberate strategy embedded in the structural dynamics of cyberspace.[12]

The MCO life-cycle is non-deterministic. Each MCO follows its own path; they can progress and regress over time, and take more or less time to transition between stages. For instance, an MCO may lose its initial operational capability or forever be stuck in the *startup* phase and never actually conduct offensive cyber operations. And if a state has a well-established signal intelligence unit, it may rely on those knowledge-structures to quickly move from the *launch* to the *growth* stage.

3. AN OVERVIEW OF NATO MEMBERS

This section offers an historical perspective of the institutional progress across members of the NATO alliance. Table II provides a baseline overview for where NATO member states currently stand in terms of MCO development, based on publicly available information.

It is hardly surprising that the United States was among the first countries in the NATO alliance that sought to conduct offensive cyber operations to achieve d4 effects. Since the 1980s there had been a growing awareness in the US of the military potential of computer attacks, according to Michael Warner, U.S. Cyber Command historian.[13] It was Operation Desert Storm, in 1991, which is said to have given further impetus to the importance of conducting military cyber operations as part of modern warfare.[14] In the US, information warfare centers were officially created by the Air Force in 1993 and a year later by the Navy and Army. In the same period, the NSA set up the Tailored Access Operations (TAO) unit.[15]

In mid-2009, Secretary of Defense Robert Gates directed the commander of U.S. Strategic Command to establish a sub-unified command, Cyber Command

[12] For an overview of potential strategic use see: Max Smeets and Herbert Lin, "Offensive Cyber Capabilities: To What Ends?" *2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects*, T. Minárik, R. Jakschis, L. Lindström (Eds.) (Tallinn: NATO CCD COE Publications: 2018); Max Smeets,"The Strategic Promise of Offensive Cyber Operations," Strategic Studies Quarterly, (2018, Fall):90-113.

[13] Rid provides a similar statement: "Defense intellectuals slowly began to discern an offensive and a defensive logic in what Post called 'cybernetic war' in 1979. This development took some time". Michael Warner, "Cybersecurity: A Pre-history", *Intelligence and National Security*, Intelligence and National Security, 27:5 (2012)781-799.

[14] For a more in-depth discussion on this, see: Ronald J. Deibert, "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," *Millennium: Journal of International Studies* (2003).

[15] For a more detailed history, see: Joint Task Force Global Network Operations, "A Legacy of Excellence: December 30, 1998- September 7, 2010", retrieved from: https://assets.documentcloud.org/documents/2849764/Document-05.pdf.

(USCYBERCOM).[16] The creation of this organization "marked the culmination of more than a decade's worth of institutional change. DoD defensive and offensive capabilities were now firmly linked, and, moreover, tied closely, with the nation's cryptologic system and premier information assurance entity, the NSA".[17] USCYBERCOM has grown significantly ever since – achieving full operational capability (133 teams) in May 2018.[18] In the same month, the Department of Defense (DoD) also elevated USCYBERCOM to a unified combatant command.[19]

Another early case – often overlooked – is that of Greece, where the government officially established an Office of Computer Warfare in 1999.[20] Five years later, in 2004, the Department of Cyber Defense was established, which was subsequently elevated to the Directorate of Cyber Defense in 2011.[21] Even though the Greek institution's development might look significant on paper, as John Nomikos writes, there is currently a lack of funding due to austerity measures, making it difficult to operate.[22] In that sense, it is unclear if the country ever passed the launch phase and actually started to conduct military cyber operations.[23]

[16] For a pre-institutional history of the U.S. Cyber Command, see United States Strategic Command, "JFT-CND/JTC-CNO/JTF-GNO: A Legacy of Excellence" (1998, December 30/ 2010, September 7), retrieved from: https://nsarchive2.gwu.edu//dc.html?doc=2849764-Document-05).

[17] Michael Warner, "U.S. Cyber Command's Road to Full Operational Capability," in *Stand Up and Fight: The Creation of U.S. Security Organizations, 1942–2005*, edited by Ty Seidule and Jacqueline E. Whitt (Carlisle, Penn.: Strategic Studies Institute and U.S. Army War College Press, 2015), chap. 7.

[18] Max Smeets and Herbert Lin, "4 A Strategic Assessment of the U.S. Cyber Command Vision," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, (Washington DC: Brookings Institution Press: 2018), pp. 81-104.

[19] Jim Garamone and Lisa Ferdinando, "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command," Department of Defense News, (2017, August 18), retrieved from: www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/.

[20] United Nations Institute for Disarmament Research (UNIDIR), "The Cyber Index International Security Trends and Realities," (2013), retrieved from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

[21] John M. Nomikos, "Intelligence Requirements for Cyber Defense, Critical Infrastructure and Energy Security in Greece," *National Security and National Future*, 1-2:17 (2016).

[22] Ibid.

[23] There are no cases of CNA publicly attributed to the Greek government.

TABLE II: OVERVIEW OF MCO DEVELOPMENT IN NATO MEMBER STATES

	Seed & Development	Start Up / Launch	Growth	Expansion	Maturity
United States	1980s	2010	2011	Present	
Estonia	2017	2017	Present		
France	2008	2011	2016	Present	
Germany	2009	2016	Present		
Italy	2014	2015	Present		
The Netherlands	2012	2015	2018		
Spain	2012	2014	Present		
Turkey	2011	2012	Present		
Belgium	2015	2019	Present		
Canada	2011	2011	2015	Present	
Denmark	2013	2017	Present		
Greece	1999	2004	Present		
Norway	2012	2012			
Poland	2008	Unknown	Unknown		
United Kingdom	2012	2012			
Portugal	2015	Unknown			

* In 2008, Poland proposed to develop an independent information force. As yet, it is unclear to what degree it is operational and focuses on OCO to achieve d4 effects; In the 2011 National Strategic Framework, Italy mentions various cyber initiatives but leaves out the development of military offensive capability.

** It remains unclear to what degree Norway's Cyber Defense branch can actually be defined as an MCO, given its narrow mission.[24]

*** There are no known MCO developments in the following NATO countries: Albania, Bulgaria, Croatia, Czech Republic, Hungary, Iceland, Latvia, Lithuania, Luxembourg, Montenegro, Slovakia and Slovenia.

Most Alliance members started to talk publicly about the need for 'cyberwarfare capabilities' in the mid-2000s. The majority are now in either the *launch* or *growth* stages. For example, the Netherlands passed the *seed* phase about eight years ago, when the Dutch government mentioned in several government publications and news articles the need to develop an offensive cyber capability to effectively 'defend and deter' other actors.[25] The government developed its political and military priorities in cyberspace through a number of official publications, including the first National Cybersecurity Strategy (2011), the Defense Cyber Strategy (2012), the second

[24] Also see: Lilly Pijnenburg Muller, "Military Offensive Cyber-Capabilities: Small-State Perspectives", Norwegian institute of International Affairs, Policy Brief, 1, (2019), retrieved from: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2583385/NUPI_Policy_Brief_1_2019_Muller.pdf?sequence=1&isAllowed=y.

[25] Strategic documents followed several parliamentary inquiries by two members of parliament (Raymond Knops and Marcial Hernandez) in 2010 and 2011.

National Cybersecurity Strategy (2013), and the Defense Cyber Strategy (2015).[26] The *startup* phase, commenced in the June 2015 when the Defense Cyber Command (DCC) was officially established. The DCC incorporates the Taskforce Cyber (TFC), established in 2012, under the Army.[27] Last year it reached the *growth* stage when it became operational, though it is known to struggle operationally.[28]

The Danish government writes in its Defense Agreement 2013-2017 that the country's "defense must have the capability for military operations in cyberspace, including the ability to protect own network infrastructure, and also to affect opponents' use of cyberspace".[29] It also explicitly states that the government should develop a "capacity that can execute defensive and offensive military operations in cyberspace".[30] In its 2012 National Cyber Security Strategy, Spain writes that one "line of action" is to "boost military and intelligence capabilities to deliver a timely, legitimate and proportionate response in cyberspace to threats or aggressions that can affect National Defence".[31] In 2011, Turkey revealed plans to establish a Cyber Command, which was officially established a year later (called the General Staff Warfare and Cyber Defense Command). At a conference in 2014, the commander of the military General Staff's Division for Electronic Systems and Cyber Defense said that Turkey considers "cyber" to be the "fifth military domain".[32]

For a long time the British government was coy in public about the offensive operations it sought to conduct and the doctrine it was following. Since 2012 this has started to change.[33] The National Cyber Security Strategy 2016-2021 is unequivocal about Britain's ambitions in this new domain. It states that: "Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere".[34] The UK aims to become "a world leader in offensive cyber capability; and […] to establish "a

[26] For an excellent overview see: Paul Ducheine, "Defensie in het digitale domein," *Militaire Spectator*, 186:4 (2017)152-168.

[27] One could potentially argue that the startup phase already started in 2012 with the establishment of the Taskforce Cyber.

[28] Liza van Lonkhuyzen and Kees Versteegh, "Het cyberleger kan en mag nog weinig," *NRC* (2018, December 18), retrieved from: https://www.nrc.nl/nieuws/2018/12/18/het-cyberleger-is-er-wel-maar-mag-weinig-a3099254.

[29] The report also mentions that: "Focus on transverse planning and deployment of capabilities, challenges in the Arctic and in cyberspace, as well as the adaptation of not least the army, will dominate the development of the defense". See: The Danish Ministry of Defense, "Danish Defense Agreement 2013-2017", (2012, November 30), retrieved from: http://www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf, p. 4 and p.8.

[30] Ibid, p. 16.

[31] Rajoy Brey, "National Cyber Security Strategy of Spain," (2013), retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf, p.32.

[32] United Nations Institute for Disarmament Research (UNIDIR), "The Cyber Index International Security Trends and Realities".

[33] Since 2012, the Joint Forces Command has taken the lead in integrating and conducting offensive cyber operations.

[34] UK government, "Britain's cyber security bolstered by world-class strategy," (2016, November 1), retrieved from: https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy.

pipeline of skills and expertise to develop and deploy our sovereign offensive cyber capabilities".[35]

It is not always easy to delineate the *seed* and *development* from the *startup* phase. In some countries, overlapping organizations were created or reorganized over the course of several years. For example, in 2011, Canada set up the Directorate of Cybernetics to "build cyberwarfare capabilities" for the armed forces.[36] But, as James Lewis notes, earlier "[t]he Canadian Armed Forces Information Management Group [was] responsible for the protection of the armed forces' computer and communications networks" with subsidiary organizations including "the Canadian Forces Network Operation Centre as well as a centre for electronic warfare and signals intelligence".[37]

Another potentially ambiguous case is France. Bernard Barbier, the former director of France's external intelligence agency (Directorate-General for External Security), said at a university lecture that the country had already explored conducting espionage operations in the early 1990s and quickly moved on to also think about warfare applications.[38] Yet the French only publicly talked about the potential conduct of military cyber operations in 2008, in a White Paper under then President Nicolas Sarközy.[39] However, as Arthur Laudrain notes, France has from 2016-2019 "conceptualized and adopted a comprehensive cybersecurity and cyber defense model".[40] In late 2016, the then-Minister of Defense Jean-Yves Le Drian announced the creation of a new cyber defense command (COMCYBER) predicted to employ 2,500 personnel by 2019 and receiving an initial commitment of €2.1 billion in funding,.[41] In 2017, the Strategic Review for Defense and National Security was published recognizing cybersecurity and 'digital sovereignty' as top priority.[42] In February 2018, France published its first National Strategy for Cyber Defense clarifying how cyber operations are organizationally integrated as well as the legal framework surrounding their use. And

[35] Ibid.

[36] Matteo Gramaglia, Emmet Tuohy, Piret Pernik. "Military Cyber Defense Structures of NATO Members," The Star, (2016, January 9), retrieved from: https://www.thestar.com/news/canada/2016/09/01/former-electronic- spy-chief- urges-ottawa-to- prepare- for-cyber- war.html ; Alex Boutilier, "Canada developing arsenal of cyber-weapons," The Star, (2017, March 16), retrieved from: https://www.thestar.com/news/canada/2017/03/16/canada-developing-arsenal-of-cyber-weapons.html;.

[37] United Nations Institute for Disarmament Research (UNIDIR), "The Cyber Index International Security Trends and Realities".

[38] Henri Chain, "Espionnage et cybersécurité, Bernard Barbier reçu par Symposium CentraleSupélec," (2016, September 5), retrieved from: https://www.youtube.com/watch?v=s8gCaySejr4.

[39] Nicolas Sarközy, "The French White Paper on Defence and National Security", (New York: Odile Jacob Publishing Corporation: 2008), retrieved from: http://www.mocr.army.cz/images/Bilakniha/ZSD/French%20White%20Paper%20on%20Defence%20and%20National%20Security%202008.pdf;.

[40] Arthur Laudrain, "France's New Offensive Cyber Doctrine," (2019, February 26), *Lawfare*, retrieved from: https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine.

[41] France has previously developed espionage platform Animal Farm. As yet, there is no public report indicating the country is conducting CNA operations. Tom Reeve, "France unveils cyber command in response to 'new era in warfare' ," *SC magazine*, (2016, December 16), retrieved from: https://www.scmagazineuk.com/france-unveils-cyber-command-in-response-to-new-era-in-warfare/article/579671/.

[42] République Française "Strategic Review of Defense and National Security: Key Points," (2017) retrieved from: https://www.defense.gouv.fr/content/download/514686/8664672/file/2017-RS-PointsClesEN.pdf.

in January 2019, France unveiled its first offensive cyber doctrine, marking another crucial milestone.[43]

This means that France and Germany stand out for the extent of resources allocated to their MCOs. In 2016, Germany outlined a plan for a cyber command said to have 13,500 personnel.[44]

Estonia is renowned for its active cybersecurity policy. For a long time, the government did not seem interested in conducting offensive cyber operations.[45] In October 2018, however, the Estonian government announced that they had established a military cyber command.[46] We can expect several other newcomers in the near future. For example, according to the Belgian media, "the Belgian military forces are to get a new [cyber] component as from 2019".[47]

4. A CLOSER LOOK AT MCO DEVELOPMENT

The above section provided a general overview of NATO member states' paths towards conducting offensive cyber operations. The purpose of this section is to highlight several additional observations.

First, MCOs do not emerge in a political and organizational vacuum. Indeed, they are often established based on rebranding, restructuring, or combining existing institutions. This means that MCO development in theory (and how it is presented in official documents) and in practice do not always closely match.

Second, it is unclear if *any* MCO is at the *maturity* stage. USCYBERCOM is undoubtedly the main candidate. Whilst its organizational structure is no longer embryonic, it cannot be described as mature. As said, USCYBERCOM only recently became a unified combatant command and achieved full operational capability. It is

[43] COMCYBER & Ministère des Armées, "Éléments publics de doctrine militaire de lutte informatique offensive," (2019), retrieved from: https://www.defense.gouv.fr/content/download/551555/9394645/Eléments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf
Also see: William Moray, "France bolsters cyber capabilities and commitment through new doctrine," *Jane's Intelligence Review* (2019, February 26).

[44] Germany has a strategic reconnaissance unit in the Department of Information and Computer Networks Operations since 2009; John Goetz, Marcel Rosenbach, and Alexander Szandar, "War of the future: national defense in cyberspace", Spiegel Online, (2009, February 11), retrieved from: http://www.spiegel.de/international/ germany/war-of-the-future-national-defense-in-cyberspace-a-606987.html; The Federal Government of Germany, "White Paper on German Security Policy and the Future of the Bundeswehr," (2016), retrieved from: http://www.new-york-un.diplo.de/contentblob/4847754/Daten/6718448/160713weibuchEN.pdf; Nina Werkhäuser, "German army launches new cyber command," DW, (2017, April 1) retrieved from: https://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517.

[45] Also, the Estonian Cyber Defence Unit (volunteer group) does not conduct CNA.

[46] Its establishment was announced a year earlier.

[47] Michael Torfs, "Belgian army to get new component to tackle cyber crime," (2017, April 7), *Flanders News*.

also still trying to strategically navigate the threat landscape – striving to end its heavy reliance on the NSA and stand on its own two feet.[48] In other words, there is still progress to be made in aligning the Cyber Command's ends, ways and means.

Third, whilst some states have devoted substantial budgets to their MCOs (which might in part be due to the broader mission and functioning requirements of the organization), most aspiring NATO cyber powers still have a rather small budget at their disposal. According to the *Wall Street Journal*, the Danish government "allocates about $10 million a year for 'computer-network operations,' including defense and offense, since 2013".[49] Other media reports indicate that, in 2015, $75 million was allocated for offensive cyber capabilities through 2017. In 2014, Spain for the first time allocated a budget of €2.3 million to enhance its ability to conduct offensive cyber operations.[50] In the Netherlands, the initial budget was €50 million to establish the new cyber command, with an annual budget around €20 million for the following years.[51] Considering the size of these budgets, it is unclear if these MCOs could ever go past the initial *growth* stage.

Fourth, there is a widely-held notion that establishing an MCO and conducting offensive cyber operations is cheap or easy. This is not the case. As an MCO moves through the stages of the life cycle, it will have to address different problems. First, the determining factor of an MCO – at any stage of the life cycle – is, as one military commander put it, "people, people, people".[52] Second, MCOs also need to acquire (or develop) toolsets in order to gain, escalate and maintain access to targeted computer systems and networks.[53] Whilst much public attention is paid to states' stockpiling of zero-day exploits, known exploits (and social engineering techniques) are unlikely to be found gathering dust at the bottom of an MCO's toolbox – even for more well-established military organizations. Third, an MCO may have the best cyber force in the world, but it is bound to fail without strategic guidance and organizational coordination. One critical issue for an MCO is to ensure that offensive cyber operations can be deployed as an integral part of the overall mission. This means that organizational coordination across the life cycle is essential to ensure interoperability.[54] This may help to explain

[48] Sulmeyer, "Much Ado About Nothing?"

[49] Jennifer Valentino-Devries and Danny Yadron, "Cataloging the World's Cyberforces," *Wall Street Journal* (2015, October 11), retrieved from: http://graphics.wsj.com/world-catalogue-cyberwar-tools/.

[50] Brey, "National Cyber Security Strategy of Spain," (2013), p. 32.

[51] Max Smeets, "People, People, People: Vragen over het DDC en het inzetten van cyberactiviteiten," *Atlantische Commissie*, (2018, April), retrieved from: https://www.atlcom.nl/upload/AP_6_2018_Smeets.pdf; Also see: van Lonkhuyzen & Kees, "Het cyberleger kan en mag nog weinig".

[52] Senior Military Cyber Commander, "The Second International Cyber Symposium: Cyberspace and the Transformation of 21st Century Warfare," The Royal United Services Institute (RUSI) (Church House, Westminster: London), 19-20 October 2016.

[53] A common distinction made is between exploits and implants (tools).

[54] For a more detailed analysis of the organizational challenges related to integration see: Michael Sulmeyer, "Much Ado about Nothing? Cyber Command and the NSA," *War on the Rocks*, (2017, July 19), https://warontherocks.com/2017/07/much-ado-about-nothing-cyber-command-and-the-nsa/; Max Smeets, "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks," 2017 9th International Conference on Cyber Conflict: Defending the Core, H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.) (Tallinn: NATO CCD COE Publications: 2017).

why so many states are still only at the early stages of development; why reports have been published in a number of states about operational struggles; and why we have publicly observed CNA-activity by only a small group of NATO member states.

Fifth, this overview of organizational development across NATO Member States is only based on *publicly* available information. It is expected that there are more institutional developments hidden from the public eye. Several states recognize the cyber threat as a priority issue, but do not seem to promote the establishment of an MCO. For example, Lithuania considers cyberspace to be a new "environment of warfighting" and recognizes the cyber threat, yet there is no evidence to suggest that the government has established a program to conduct offensive cyber operations to achieve d4 effects. A similar discussion is provided in the 2015 Security Strategy of the Czech Republic and the cyber strategy of the Slovak Republic.[55] It would be hardly surprising if some of these states are in fact considering conducting military cyber operations.

5. CONCLUDING REMARKS

The aim of this paper was to provide a conceptual framework to facilitate analysis and comparison between different MCOs across NATO member states. The life cycle framework distinguishes between five stages of organizational development: i) seed, ii) startup, iii) growth, iv) expansion, and v) maturity.

It was shown that a large number of NATO Member States started to carefully consider establishing MCOs from 2008 onwards, and some had already started significant organizational efforts in the 1990s. However, I also reveal that the MCOs of most NATO members are still at the early stages of organizational development – and even those at the growth stage still have limited budgets to address the different workforce, capability, strategic and other requirements.

Future research can fruitfully expand this analysis on the MCO life cycle in a number of ways. As an MCO moves through the stages, a government faces different organizational challenges. I did not assess how different governments have sought to overcome these challenges. Also, it remains unclear to what degree governments can help each other in MCO development through international cooperation with other like-minded states – within or outside the NATO alliance. Also, more attention should

[55] National Security Authority, "National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020," (2015), retrieved from, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf; Peter Pellegrini and Robert Fico, "Cyber Security Concept of the Slovak Republic for 2015 - 2020," retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1; Also see: Tomáš Minárik, "National Cyber Security Organisation: Czech Republic," CCD COE Publications, 2nd version, (2016), retrieved from: https://ccdcoe.org/uploads/2018/10/CS_organisation_CZE_032016.pdf.

be paid to the benefits and limitations of bringing in private sector solutions. Finally, we could benefit from more case study research, process tracing organizational decisions and capturing other developments, and looking at countries' progress in more detail.

REFERENCES

Arts, Sophie "Offense as the New Defense: New Life for NATO's Cyber Policy," *The German Marshall Fund of the United States, Policy Brief*, 39, (2018):1-9.

Boutilier, Alex, "Canada developing arsenal of cyber-weapons," *The Star*, (2017, March 16), retrieved from: https://www.thestar.com/news/canada/2017/03/16/canada-developing-arsenal-of-cyber-weapons.html;

Brey, Rajoy, "National Cyber Security Strategy of Spain," (2013), retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf

Chain, Henri, "Espionnage et cybersécurité, Bernard Barbier reçu par Symposium CentraleSupélec," (2016, September 5), retrieved from: https://www.youtube.com/watch?v=s8gCaySejr4

Churchill, Neil C., and Virginia L. Lewis, "The Five Stages of Small Business Growth," *Harvard Business Review*, (1983, May), retrieved from: https://hbr.org/1983/05/the-five-stages-of-small-business-growth

COMCYBER & Ministère des Armées, "Éléments publics de doctrine militaire de lutte informatique offensive," (2019), retrieved from: https://www.defense.gouv.fr/content/download/551555/9394645/Eléments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf

Deibert, Ronald J.,"Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," *Millennium: Journal of International Studies* (2003).

Ducheine, Paul "Defensie in het digitale domein," *Militaire Spectator*, 186:4 (2017)152-168.

Dutch Ministry of Defense, Third International Cyber Operations Symposium, (2017, October);

Garamone, Jim, and Lisa Ferdinando, "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command," *Department of Defense News*, (2017, August 18), retrieved from: www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/)

Goetz, John, Marcel Rosenbach, and Alexander Szandar, "War of the future: national defense in cyberspace", *Spiegel Online*, (2009, February 11), retrieved from: http://www.spiegel.de/international/ germany/war-of-the-future-national-defense-in-cyberspace-a-606987.html

Gramaglia, Matteo, Emmet Tuohy, Piret Pernik. "Military Cyber Defense Structures of NATO Members," *The Star*, (2016, January 9), retrieved from: https://www.thestar.com/news/canada/2016/09/01/former-electronic- spy-chief- urges-ottawa-to- prepare- for-cyber- war.html

Joint Task Force Global Network Operations, "A Legacy of Excellence: December 30, 1998- September 7, 2010", retrieved from: https://assets.documentcloud.org/documents/2849764/Document-05.pdf

Laudrain, Arthur, "France's New Offensive Cyber Doctrine," (2019, February 26), Lawfare, retrieved from: https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine

Minárik, Tomáš , "National Cyber Security Organisation: Czech Republic," CCD COE Publications, 2nd version, (2016), retrieved from: https://ccdcoe.org/uploads/2018/10/CS_organisation_CZE_032016.pdf

Moray, William, “France bolsters cyber capabilities and commitment through new doctrine,” *Jane’s Intelligence Review* (2019, February 26).

National Security Authority, “National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020,” (2015), retrieved from, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

NATO, “Brussels Summit Declaration, (2018, July 11-12), retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-summit-declaration-eng.pdf

Nomikos, John M., “Intelligence Requirements for Cyber Defense, Critical Infrastructure and Energy Security in Greece,” *National Security and National Future*, 1-2:17 (2016).

Pellegrini, Peter and Robert Fico, “Cyber Security Concept of the Slovak Republic for 2015 – 2020,” retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1

Pernik, Piret, “Preparing for Cyber Conflict: Case Studies of Cyber Command,” (2018, December), retrieved from: https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf

Petch, Neil, “The Five Stages Of Your Business Lifecycle: Which Phase Are You In?” *Entrepreneur*, (2016, February 29), retrieved from: https://www.entrepreneur.com/article/271290

Pijnenburg Muller, Lilly, “Military Offensive Cyber-Capabilities: Small-State Perspectives, Norwegian Institute of International Affairs, Policy Brief, 1, (2019), retrieved from: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2583385/NUPI_Policy_Brief_1_2019_Muller.pdf?sequence=1&isAllowed=y

Reeve, Tom, “France unveils cyber command in response to ‘new era in warfare’ ,” SC magazine, (2016, December 16), retrieved from: https://www.scmagazineuk.com/france-unveils-cyber-command-in-response-to-new-era-in-warfare/article/579671/

République Française “Strategic Review of Defense and National Security: Key Points,” (2017) retrieved from: https://www.defense.gouv.fr/content/download/514686/8664672/file/2017-RS-PointsClesEN.pdf

Sarközy, Nicolas, “The French White Paper on Defense and National Security”, (New York: Odile Jacob Publishing Corporation: 2008), retrieved from: http://www.mocr.army.cz/images/Bilakniha/ZSD/French%20White%20Paper%20on%20Defence%20and%20National%20Security%202008.pdf

Schulze, Matthias and Sven Herpig, “Germany Develops Offensive Cyber Capabilities Without a Coherent Strategy of What to Do With Them,” Council on Foreign Relations, (2018, December 3), retrieved from: https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them

Senior Military Cyber Commander, “The Second International Cyber Symposium: Cyberspace and the Transformation of 21st Century Warfare,” The Royal United Services Institute (RUSI) (Church House, Westminster: London), 19-20 October 2016.

Sheldon, John B., “NATO and Cyber Defense: Hanging Together or Hanging Separately?”, Presentation, (year unknown), hxxp://www.unidir.ch/files/conferences/pdfs/nato-and-cyber-defence-hanging-together-or-hanging-separatelyen-1-608.pdf

Smeets, Max, and Herbert Lin, “4 A Strategic Assessment of the U.S. Cyber Command Vision,” in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, (Washington DC: Brookings Institution Press: 2018), pp. 81-104.

Smeets, Max, “Going cyber : the dynamics of cyber proliferation and international security,” DPhil Dissertation in International Relations, University of Oxford, 2017.

Smeets, Max, “Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks,” *2017 9th International Conference on Cyber Conflict: Defending the Core*, H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.) (Tallinn: NATO CCD COE Publications: 2017).

Smeets, Max, and Herbert Lin, “Offensive Cyber Capabilities: To What Ends?” *2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects*, T. Minárik, R. Jakschis, L. Lindström (Eds.) (Tallinn: NATO CCD COE Publications: 2018).

Smeets, Max, “The Strategic Promise of Offensive Cyber Operations,” *Strategic Studies Quarterly*, (2018, Fall):90-113.

Smeets, Max “People, People, People: Vragen over het DDC en het inzetten van cyberactiviteiten,” *Atlantische Commissie*, (2018, April), retrieved from: https://www.atlcom.nl/upload/AP_6_2018_Smeets.pdf

Sulmeyer, Michael, “Much Ado about Nothing? Cyber Command and the NSA,” *War on the Rocks*, (2017, July 19), https://warontherocks.com/2017/07/much-ado-about-nothing-cyber-command-and-the-nsa/

The Danish Ministry of Defense, “Danish Defense Agreement 2013-2017”, (2012, November 30), retrieved from: http://www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf

The Federal Government of Germany, “White Paper on German Security Policy and the Future of the Bundeswehr,” (2016), retrieved from: http://www.new-york-un.diplo.de/contentblob/4847754/Daten/6718448/160713 weibuchEN.pdf

Torfs, Michael, “Belgian army to get new component to tackle cyber crime,” (2017, April 7), *Flanders News*.

UK Government, “Britain’s cyber security bolstered by world-class strategy,” (2016, November 1), retrieved from: https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy

United Nations Institute for Disarmament Research (UNIDIR), “The Cyber Index International Security Trends and Realities,” (2013), retrieved from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

United States Strategic Command, “JFT-CND/JTC-CNO/JTF-GNO: A Legacy of Excellence” (1998, December 30/ 2010, September 7), retrieved from: https://nsarchive2.gwu.edu//dc.html?doc=2849764-Document-05)

US Department of Defense, “News Conference By Secretary Mattis at NATO Headquarters, Brussels, Belgium,” US Department of DEcen, (2018, October 4), retrieved from: dod.defense.gov

Valentino-Devries, Jennifer, and Danny Yadron, “Cataloging the World’s Cyberforces,” *Wall Street Journal* (2015, October 11), retrieved from: http://graphics.wsj.com/world-catalogue-cyberwar-tools/

Van Lonkhuyzen, Liza and Kees Versteegh, “Het cyberleger kan en mag nog weinig,” *NRC* (2018, December 18), retrieved from: https://www.nrc.nl/nieuws/2018/12/18/het-cyberleger-is-er-wel-maar-mag-weinig-a3099254

Warner, Michael, “Cybersecurity: A Pre-history”, Intelligence and National Security, *Intelligence and National Security*, 27:5 (2012)781-799.

Warner, Michael, “U.S. Cyber Command’s Road to Full Operational Capability,” in Stand Up and Fight: The Creation of U.S. Security Organizations, 1942–2005, edited by Ty Seidule and Jacqueline E. Whitt (Carlisle, Penn.: Strategic Studies Institute and U.S. Army War College Press, 2015), chap. 7.

Werkhäuser, Nina, “German army launches new cyber command,” DW, (2017, April 1) retrieved from: https://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517