Organizing cyber capability across military and intelligence entities

Collaboration, separation, or centralization

Liebetrau, Tobias

Published in:
Policy Design and Practice

DOI:
10.1080/25741292.2022.2127551

Publication date:
2023

Document license:
CC BY

Citation for published version (APA):
Organizing cyber capability across military and intelligence entities: collaboration, separation, or centralization

Tobias Liebetrau

To cite this article: Tobias Liebetrau (2022): Organizing cyber capability across military and intelligence entities: collaboration, separation, or centralization, Policy Design and Practice, DOI: 10.1080/25741292.2022.2127551

To link to this article: https://doi.org/10.1080/25741292.2022.2127551

© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

Published online: 29 Sep 2022.

Article views: 1334

View related articles

View Crossmark data
Organizing cyber capability across military and intelligence entities: collaboration, separation, or centralization

Tobias Liebetrau

ABSTRACT

This paper explores how the Netherlands, France, and Norway organize their cyber capabilities at the intersection of intelligence services and military entities and provides recommendations for policy and research development in the field. Drawing out key organizational differences and ambiguities, the analysis identifies three models of organizing military and intelligence relations: A Dutch collaboration model, a French separation model, and a Norwegian centralization model. Despite their divergence in organizing cyber capabilities, the three countries converge on the assumption that both responding to cyber conflict short of war and developing military cyber power are dependent on the skills, information, and infrastructure of intelligence services. This calls for cooperation and coordination across military and intelligence entities. However, it remains unclear whether decision makers have systematically assessed the implications of the organizational structure for the ways in which the two dimensions relate to and shape one another at strategic, tactical, and operational levels. The paper concludes that there is a need for increased political attention and a deliberate approach to how the organizational model allows for the operational cyber capacity to travel from, translate into, and shape intelligence and military entities and to which political implications at both national and international levels.

ARTICLE HISTORY

Received 7 May 2022
Accepted 14 September 2022

KEYWORDS

Cybersecurity; cybersecurity governance; European security; cyber capability; conflict short of war; cyber operations

Recent cyber incidents such as the SolarWinds, the Microsoft Exchange, and the Colonial Pipeline hacks demonstrate how malicious cyber operations continue to question the demarcation lines between war and peace, military and civilian, and internal and external security. Existing scholarship has documented how European countries (Liebetrau 2022) and NATO (Jacobsen 2021) struggle to address such cyber aggressions below the threshold of war. This article advances this debate by undertaking a comparative analysis of how the Netherlands, France, and Norway organize their cyber capabilities at the intersection of intelligence services and military entities. The
paper thereby sheds light on a pressing cybersecurity policy and governance issue that has received scarce political and academic attention. It offers scrutiny of the challenges and opportunities faced by European countries when organizing their cyber capabilities and provides recommendations for policy development in the field.

Burton and Christou (2021, 1727) observe how more and more international actors develop and use “offensive cyber tools for a broad range of strategic purposes, including espionage, subversion, coercion, war-fighting and hybrid warfare campaigns”. Accordingly, cybersecurity research is increasingly guided by the “empirical reality of persistent cyber operations across the conflict spectrum” (Cavelty and Wenger 2020, 16). Yet, the scholarly and political debate about the organization of cyber capabilities “has been dominated by U.S. voices and U.S. issues” (Devanny and Stevens 2021). The academic literature has paid scarce attention to how European countries organize cyber capabilities at the intersection of military cyber commands and intelligence services. It is, however, crucial to examine and assess the organization of cyber capabilities if we are to better understand the practical, political, and democratic implications of engaging with the current challenges that persistent cyber operations short of war as well as military cyber operations in armed conflict amount to.

This paper relies primarily on written public sources, such as official government statements and publications, media reports, and academic literature. These documents are supported by interviews with military personnel, civil servants, and scholars in the three countries. The article demonstrates how military-intelligence relations vary across the countries and identifies three organizing models: a Dutch collaboration model, a French separation model, and a Norwegian centralization model. It also shows that the three countries seem to converge on the fact that both the countering of cyber conflict short of war and the development of military cyber capabilities are dependent on the skills, information, and infrastructure of intelligence services. However, it is unclear whether decision makers have systematically assessed how the organizational model allows for the operational capacity to travel from, translate into, and shape intelligence and military entities and to which strategic and governance implications. This creates risks that operational capability and activity may be mismatched with broader strategic or governance goals, that the military and intelligence entities operate with different purposes and goals, that political decision-making is hampered, and that democratic oversight is hindered.

Given the secrecy and confidentiality that shroud the topic and the lack of existing studies, the conclusions of this piece are to be considered tentative. Drawing out these three models of organizing cyber capabilities and their dominant characteristics, should be considered a starting point for further explorations and discussions of how European countries can and ought to organize their cyber capabilities across intelligence and military entities. The observed divergence in organizing cyber capabilities is likely to be explained by multiple factors, including strategic posture, military culture, economic and human resources, and political will and attention. While future research could examine these and other explanatory factors, it is paramount that researchers and policy makers devote greater attention to the organizing of cyber capabilities, including the operational and strategic implications of the organizational divergence across NATO and EU members. This applies to coping with the challenges of
persistent cyber conflict short of war as well as the application of cyber operations in armed conflict.

The paper proceeds by locating the study in relation to relevant debates in cybersecurity scholarship. It then examines the organization of cyber capabilities across military and intelligence entities in the Netherlands, France, and Norway. The final section concludes and offers recommendations for future academic and policy debate and design.

Organizing cyber capability between military and intelligence

While much of the US-driven academic debate has focused on if and how cyber operations reach the threshold of war, this paper focuses on the organizing of offensive capabilities between military and intelligence in Europe. In doing so, it speaks to four strands of cybersecurity literature touching upon military and intelligence entities. First, scholars have pointed out that the central (state) actors conducting cyber operations are intelligence agencies, and deceptive cyber operations, therefore, form part of an intelligence contest (Gartzke and Lindsay 2015; Rovner 2020). A related, yet alternative, argument is brought forward by supporters of cyber persistence theory. They suggest that “strategy must be unshackled from the presumption that it deals only with the realm of coercion, militarised crisis, and war in cyberspace” (Harknett and Smeets 2022, 2). They argue that “strategic outcomes in, through and from cyberspace are possible short of war” (Michael and Harknett 2020, 1).

Second, scholars have shown that boundary drawing between intelligence and military cyber operations is extremely challenging for at least three reasons. First, cyber operations are often custom-made combinations of intelligence, intrusion, and attack (Smeets 2018). It is seldom distinct where one stage ends, and another begins. Second, there is much ambiguity related to attribution, intention, and effect of cyber operations (Buchanan 2016). This includes political and legal questions of when exactly an offensive cyber operation can be regarded as a use of force. Third, we have witnessed an expansion of intelligence activities beyond traditional espionage, with tasks and responsibilities ranging from protecting government networks to executing offensive cyber operations abroad (Gioe, Goodman, and Stevens 2020).

Third, a literature on cybersecurity governance has examined how different models of public–private partnerships shape cyber crisis management (Boeke 2018a), how states navigate between functional and national security imperatives to design governance arrangements (Weiss and Jankauskas 2019), what governance requirements transboundary cyber crisis entail (Backman 2021), and how a Central Cyber Authority (CCA) can help structure national cyber defense (Matania, Yoffe, and Goldstein 2017). This strand of literature is focused on cyber defense arrangements and does not speak directly to the organizing of offensive cyber capabilities across military and intelligence entities.

Fourth, in the US context, we have seen continuous debate about the dual-hat arrangement concerning the NSA and the US Cyber Command (Chesney 2020; Demchak 2021), and Lindsay (2021) has recently examined and criticized the organization of the US Cyber Command. Cybersecurity scholarship has also investigated the organization of both military cyber entities (Pernik 2020, Smeets 2019) and offensive
cyber capabilities (Smeets 2018). This scholarship is, however, guided by crafting conceptual frameworks (Smeets 2018, 2019) or mapping the development of cyber commands (Pernik 2020). Systematic attention has been less devoted to comparative empirical studies of the specific organization of cyber capabilities across military and intelligence agencies in European countries. This article provides a first step in closing that gap by offering a dedicated perspective on the organization of offensive cyber capabilities across three European countries.

This article refers to offensive cyber capabilities as custom-made combinations of human and non-human elements that allow cyber operations to achieve impact across the spectrum of intelligence and attack. The development and deployment of these cyber capabilities weave together strategic guidance, legal mandate, doctrinal procedures, human skills, technological capacity, and organizational arrangement (see also Slayton 2017, Smeets 2022). This broad perception of offensive capabilities is deliberately chosen to allow for the empirics to speak rather than an overly restrictive pre-given conceptualization. Following the same line of thinking, this article offers a comparative exploratory qualitative analysis (Yin 2014) of how the development and deployment of cyber capabilities are structured across military cyber commands and foreign intelligence services in the Netherlands, France, and Norway. The exploratory nature of the study ensures an empirical sensitivity in line with understanding cybersecurity as a situated and contextual object of study, rather than being predetermined by the existing theories and categories (Liebetrau and Christensen 2021).

The selection of the three countries rests on a combination of pragmatic reasoning in terms minimizing the language barrier and achieving access to interviewees, and the fact that the countries represent a large-, a medium-, and a small-sized European country with ambitious cybersecurity policies and long-term publicly declared ambitions of developing offensive cyber capabilities. As paradigmatic cases they were not chosen because of e.g. extremity, deviancy, or similarity, but because they highlight more general characteristics of the organization of cyber capabilities in Europe (Flybjerg 2006). Characteristics that are not meant to be fully comparable or generalizable, but rather to be discussed, explored, and questioned in future empirically driven research on the development and deployment of cyber capabilities in Europe. Consequently, the paper neither provides an exhaustive conceptualization of the organization of cyber capabilities, nor a set of fully fledged policy prescriptions of the requirements for intelligence services or military cyber commands to conduct specific cyber operations. Instead, it aims for the empirical analysis to provoke and open up academic and policy discussions on the practical, political, and democratic implications of the organizational aspect of developing and deploying cyber capabilities, while keeping in mind its entanglements.

**The Netherlands: organizational collaboration**

In the past decade, the defense cybersecurity strategies of the Netherlands have displayed the nation’s ambition to develop offensive cyber capabilities (Bunk and Smeets 2021; Claver 2018). In 2014, the Netherlands established a Defence Cyber Command (DCC), with the aim to strengthen the country’s defense and offense in the cyber
domain. The DCC, located under the commander-in-chief of the Dutch Armed Forces since 2018, became operational by the end of 2015 (Ducheine, Arnold, and Peter 2020). The DCC concentrates on establishing and deploying defensive, intelligence, and offensive cyber capabilities. In this context, the DCC sees offensive cyber capabilities as digital resources the purpose of which is to influence or pre-empt the actions of an opponent by infiltrating computers, computer networks and weapons and sensor systems so as to influence information and systems. The Netherlands Defence organisation deploys offensive digital resources exclusively against military targets.

The mission of the DCC is to carry out offensive cyber operations in the context of armed conflict and war and act as a potential deterrent measure in time of peace (Ministry of Defense 2015, 2018). The DCC does not have mandate to play an active role in disrupting continuous adversarial cyber behavior short of war. The operational capability of the DCC is, however, hampered by its limited mandate that restricts the DCC’s possibility to gather intelligence and conduct reconnaissance when not in war. This not only makes it difficult to select and impact targets, but it also makes it hard to attract and maintain the necessary human skills (Smeets 2021). According to interviewees, the DCC lacks the necessary human expertise and technical infrastructure to carry out offensive cyber activities on its own. Hence, the DCC is primarily able to act as “coordinator and operational hub” when it comes to the deployment of Dutch offensive cyber operations in armed conflict (Claver 2018, 169). At the time of writing, there is no public information that the DCC has conducted offensive cyber operations.

On the contrary, the Military Security and Intelligence Service (MIVD) has demonstrated significant operational cyber capacity in several cases. Some of its work is undertaken in collaboration with the General Intelligence and Security Service (AIVD) in the Joint SIGINT Cyber Unit (JSCU). As a collaboration between the MIVD and the AIVD, the JSCU forms a cornerstone of the Dutch cybersecurity. The primary tasks of the unit are the collection of signal intelligence and the delivery of intelligence through cyber operations. The MIVD and JSCU are therefore crucial partners for the DCC. It is not publicly disclosed how the human and technical infrastructure resources are pooled in the event of a cyber-attack on the Netherlands surmounting to armed conflict.

The collaboration between the DCC and MIVD/JSCU raises strategic and legal issues as the MIVD and JSCU operate under different political and legal mandates. As part of the intelligence community, the MIVD is placed under the Secretary-General of the Ministry of Defense. In addition, the MIVD does not conduct military operations. Instead, its operations are based on a specific intelligence services legislation. The legal framework does allow MIVD to conduct counter-operations. As stressed by Claver (2018, 168), “all three organizations are very different in procedures, operating style, tasks, and outlook”. According to Sergie Boeke (2018, 28), it hampers the effectiveness and execution of Dutch cyber power that intelligence and military operations operate on different mandates, cultures, and methods of working. Moreover, it spurs the risk that the operational capability and activity of intelligence and military entities are mismatched with the broader strategic or governance goals.
The Netherlands presented a military cyber doctrine in 2019. The doctrine calls for increased coordination and collaboration between the Cyber Command and the intelligence services. It stresses that the difference between the conduct of cyber operations in war and for espionage relates to the purpose and the desired effect and underlines that those cyber capabilities are complementary and non-competing (Defence Cyber Command 2019, 14–15). Along the same line, the Ministry of Defense emphasizes, in its ‘Defence Vision 2035: Fighting for a safer future’, the need for organizational decompartmentalization when countering hybrid threats in the information environment (Ministry of Defense 2020, 17) and promises to devote attention to the hybrid strategic competition between war and peace (Ministry of Defense 2020, 23). However, the documents do neither elaborate on the organizational collaboration between the Cyber Command and the intelligence services nor how cyber operations are meant to complement each other at the strategic, tactical, or operational levels.

The analysis of the Dutch organization of cyber capabilities shows organizational separation between the DCC – which can deploy cyber capabilities in the event of armed conflict and war – and the intelligence services that can deploy cyber capabilities for intelligence and active defense purposes. While the Dutch model strongly notes the need for collaboration between the DCC and the intelligence services, it remains ambiguous how they complement each other in practice and how organizational collaboration is supposed to fulfill goals of increased effectiveness, synergy, and flexibility. This raises concern that the operational cyber capability of the Netherlands is hampered by the current organizational structure and legal mandate.

France: organizational separation

A key pillar in the organization of French cyber capabilities is a governance model that separates offensive missions and capabilities from defensive missions and capabilities (Desforges 2022; Liebetrau 2022). This was recently recalled, and contrasted with the Anglo-Saxon model, in the landmark 2018 Cyber Defense Strategic Review, drawn up under the authority of the General Secretariat for Defense and National Security (SGDSN). As part of this clarification, the strategic review formalizes four operational cyber chains and consolidates their governance. These are protection, military action, intelligence, and judicial investigation (Secrétariat général de la défense et de la sécurité nationale 2018, 5–6). In the following, the three first of these are deployed as starting points for examining the organization of French cyber capabilities.

The cornerstone of French cyber defense is The National Cybersecurity Agency (ANSSI). It is placed under the SGDSN and is responsible for the protection chain. The responsibilities of the agency include coordinating of the national cyber defense strategy, protecting state information networks, regulating critical infrastructure and the private sector, certifying products, and hosting the national Computing Emergency Response Team. The ANSSI is organizationally separated from the intelligence and military branch of French cybersecurity.

It has been more than a decade since France made cyberwar a national security priority and mandated the development of defensive and offensive cyber capabilities (Commission du Livre blanc sur la défense et la sécurité nationale 2008). The depiction
of cyberspace as a warfighting domain contributed to developing the role of the French Ministry of the Armed Forces in cybersecurity matters. With the 2013 military programming law, the French defense saw the establishment of the first real operational cyber defense chain (Géry 2020). In 2017 it became the cyber defense command (COMCYBER) and was placed directly under the chief of staff of the armed force. The COMCYBER is responsible for the military action chain. This includes protecting the information systems of the defense and for developing, coordinating, and deploying military cyber operations.

The deployment of cyber capabilities has a long history with the French foreign intelligence service The General Directorate for External Security (DGSE) (Guédard 2020). The DGSE is the largest French intelligence service in terms of workforce. In recent years, the DGSE has become more open about its work, but it remains a very secretive service (Chopin 2017: 546). The intelligence chain of the strategic review stresses the possibility for the implementation of offensive cyber capabilities (Secrétariat général de la défense et de la sécurité nationale 2018, 5–6). DGSE is the most important service in this regard. Yet, the review does not elaborate on when, how, or in collaboration with whom. According to Stéphane Taillat (2019), a significant part of offensive cyber operations is the responsibility of the DGSE and lies outside of the French military cyber strategy.

The organizational separation contains multiple ambiguities. First, the ANSSI can respond to a computer attack affecting the national security of France by carrying out the technical operations necessary to characterize the attack and neutralize its effects by accessing the information systems that are at the origin of the attack (Géry 2020). Depending on how this is done and interpreted, it can qualify as an offensive cyber operation.

Second, the SGDSN has declared that ANSSI will “continue to develop operational synergies with its national institutional partners”. The agency will therefore establish a branch in Rennes with the goal of “bringing it closer to the major institutional players associated with the Ministry of Defense, starting with COMCYBER” (Secrétariat général de la défense et de la sécurité nationale 2019, 29). This is in line with the strategic review’s recommendation (that has been picked up) to establish three coordinating bodies for cyber defense: le Comité directeur de la cyberdéfense, le Comité de pilotage de la cyberdéfense, le Center de coordination (C4) (Secrétariat général de la défense et de la sécurité nationale 2018, 137). Asked by the newspaper Libération about the prospect for future operational cooperation, the head of ANSSI, Guillaume Poupard, has said that “by 2025, I think we will have the obligation to have common platforms [bringing together defenders and attackers] to react effectively to the worst threats” (Amaelle 2020). While the collaboration between ANSSI, COMCYBER, and the French intelligence services is hence likely to increase, neither the desired outcome of the collaboration nor its strategic and practical dimensions are explicated.

Third, zooming in on the relationship between the COMCYBER and the intelligence services, it has been stressed that the intelligence services provide essential support to military operations by offering both technical and operational elements necessary to acquire knowledge of the adversary and operational environment (Florant 2021, 19). The French Military Cyber Strategy – that so far consists of three separate documents:
the Ministerial Policy for Defensive Cyber Warfare, the Public Elements for the Military Cyber Warfare Doctrine, and the Public Elements for Cyber Influence Warfare Doctrine (Ministère des Armées 2019a, 2019b, 2021) – does, however, not elaborate on the collaboration between the COMCYEBR and the intelligence services. Taillat (2019) finds the ambiguity to be “partly deliberate”, but stresses how it “brings to light the resulting loopholes when attempting to draw organizational boundaries in a new context of operations”.

Another potential military-intelligence loophole concerns the design and development of cyber capabilities. The COMCYBER rely on the Information Management Division of the Directorate General of Armament11 (DGA-MI) for the development and design of cyber capabilities (Ministère des Armées 2019b, 11). This collaboration is mentioned in research (Guédard 2020, Florant 2021) and journalism (Amaelle 2020) reviewing the development of French cyber capabilities. Despite the military operations need for technical and operational support from intelligence services, it is unclear what – if any – role the intelligence services play in this area.

While the principle of separation is strong on paper, the French organization of cyber capabilities is more complex. Arguably, the strict French division between defensive and offensive measures is being challenged by increased coordination and collaboration across defense, intelligence, and military institutions. This development finds support in the ‘Strategic Vision of the Chief of Defense Staff’ from October 2021. It states that the post-cold war peace-crisis-war continuum no longer applies. It has been replaced by the competition-dispute-confrontation triptych (Burkhard 2021, 8). In this new normal, the French Armed Forces must “win the war before the war” (Burkhard 2021, 13). Yet, there is very little public information on how the collaboration plays out between the ANSSI, COMCYBER, and the intelligence services. Consequently, also in the French case, it is ambiguous how the entities complement each other in practice, and how the desired organizational collaboration will achieve impact.

**Norway: organizational centralization**

The organization of Norwegian cyber capabilities rests on a centralized model. It distinguishes itself by not having a dedicated cyber command. Instead, the Norwegian military and civilian foreign intelligence service (E-tjenesten) is responsible for intelligence operations, offensive cyber operations, and for coordinating between offensive and defensive cyber operations. The 2018 intelligence law says that the service has “the national responsibility for planning and carrying out offensive cyber operations, including cyber attacks (Computer Network Attack), as well as coordinating between offensive and defensive cyber measures in the armed forces” (Forsvarsdepartementet 2018, 12).

The Norwegian Ministry of Defense (Forsvarsdepartementet 2019a, 19) describes it in the following way:

The responsibility for network intelligence operations and offensive cyberoperations are with the Intelligence Service. In military operations the Intelligence Service coordinates the activity with the Armed Forces’ operational headquarters (FOH). The Cyber Defense is responsible for conducting defensive cyber operations, and the Intelligence Service coordinates between offensive and defensive cyber operations.
The Ministry of Defense (ibid) stresses that it will “further develop the Intelligence Service’s ability to counter threats before incidents occur” and emphasize that “that cooperation and coordination between the above-mentioned actors in military cyber operations [the intelligence service and the FOH] will be strengthened, based on a military cyber operations center in the Intelligence Service”. However, the Ministry does not elaborate on how the coordination between the intelligence service and the operational headquarters plays out or what it exactly entails.

The Norwegian long-term defense plan for 2021–2024 notes that access to up-to-date and relevant information about threats and threat actors is absolutely central to being able to handle threats in the digital space (Forsvarsdepartementet 2020, 76). This underlines the importance of intelligence. The plan stresses that “the ability of the e-service [foreign intelligence service] in peace, crisis and in armed conflict to follow, attribute, warn and actively counter digital threats also before events occur, shall be further developed. The capability and competence in offensive cyber operations is to be further developed” (Forsvarsdepartementet 2020, 118). It is hence clear that the competence to deploy cyber capabilities for both intelligence and military ends lies solely with the foreign intelligence service.

But why this Norwegian particularity? Why does Norway not have a standalone cyber command? One part of the answer can be traced to the 2014 internal guideline for information security and the conduct of cyber operations in the defense (Forsvarsdepartementet 2014). Following the 2012 long-term plan for the Norwegian Armed Forces, the guideline notes that the Norwegian armed forces must have the capacity for offensive cyber operations (Forsvarsdepartementet 2014, 13). It describes both intelligence and military cyber operations as offensive actions, notes that they are usually carried out in the network of the opponent, and stresses that their execution falls under the responsibility of the chief of the intelligence service (Forsvarsdepartementet 2014, 6 and 17). Norway has kept with this model in order to foster synergies and reduce the costs of developing and deploying cyber capabilities.

In 2018, the Norwegian Ministry of Defense (Forsvarsdepartementet 2018, 8) explained, in an investment plan accepted by the government, that it is, according to the Ministry of Defense, neither necessary nor desirable to create a cyber command outside the Intelligence Service. This would, inter alia, lead to the creation of a duplication of capabilities, resulting in an unclear distinction between offensive cyber operations inside and outside military operations. A cyber command function outside the Intelligence Service will, for Norway, be an unfortunate and costly solution.

An additional argument for the centralized model was given by the Ministry of Defense in written communication with the author. The Ministry states that “the ability to carry out offensive cyber operations depends on a very good understanding of the target. It is achieved through communication intelligence and interaction with several other intelligence capabilities…” (Forsvarsdepartementet 2019b). Yet, the Ministry does neither elaborate further on the relationship between intelligence and military operations nor what the internal organizational diagram looks like.
However, under the Joint Cyber Coordination Center (FCKS), the intelligence service collaborates and coordinates with the National Security Authority (NSM), the Policy Security Service (PST), and The National Criminal Investigation Service (Kripos) when it comes to countering and dealing with severe cyber operations (Forsvarsdepartementet 2020, 76–77). Yet, as emphasized by the Norwegian Foreign Policy Institute (NUPI), “…given the high degree of secrecy around these issues, we do not know the division of labor between PST [Police Security Service], NSM [National Security Authority] and the Intelligence Service here, but it can be demanding to maintain concrete and formal distinctions between acquisition, impact operations, and security measures in the digital space”.

The Norwegian organization of cyber capabilities is founded on a centralized model that dissolves the organizational distinction between military and intelligence entities. This seems to overcome some of the challenges to organizational collaboration pointed out above, but the extent to which this is the case is hard to say, as it is unclear how intelligence and military operations complement each other in practice. There is hence a risk that many of the challenges to collaboration are internalized.

**Conclusion: future paths for policy and research**

This article has demonstrated significant divergence in organizing cyber capabilities across military and intelligence in the Netherlands, France, and Norway. Drawing out key organizational differences and ambiguities, the analysis identified three models of organizing military and intelligence relations: A Dutch collaboration model, a French separation model, and a Norwegian centralization model. Despite the divergence in organizing cyber capabilities, the three countries converge on the assumption that both responding to cyber conflict short of war and developing military cyber power are dependent on the skills, information, and infrastructure of intelligence services. This calls for cooperation and coordination across military and intelligence entities. It is, however, unclear whether decision-makers have systematically assessed the implications of the organizational structure for the ways in which the two dimensions relate to and shape one another at strategic, tactical, and operational levels. There is hence a need for increased attention and a focused approach to how the country-specific organizational model allows for operational capacity to travel from, translate into, and shape intelligence and military entities and to which implications. These elements hold the promise to decrease the risks that operational capability and activity are mismatched with broader strategic or governance goals, that the military and intelligence entities operate with different purposes and goals, and that political decision-making is hampered, and democratic oversight is disadvantaged.

The observed divergence in organizing cyber capabilities raises several questions for policy makers, practitioners, and scholars to consider. First, there is a need for political and public debate about the organization of cyber capabilities across military and intelligence entities and its relation to combating cyber hostilities short of war. Increased focus on the organizational aspects can help states to clarify and communicate their priorities and decisions when it comes to answering the questions of how, when, and who engages in cyber conflict short of war. This should be done with great sensitivity
to tangential elements of developing and deploying cyber capabilities – such as strategic guidance, legal mandate, doctrinal procedures, human skills, technological capacity – as well as the specificity of national contexts. Nurturing such debate is crucial to achieve the best decisions about how to organize and develop cyber capabilities, how to use it, and how to secure transparency and accountability.

Second, neither consistency in organizational collaboration, separation, nor centralization will automatically translate into efficient operational cyber capabilities to be deployed in intelligence contest, strategic competition, or military confrontation. Organizing cyber capabilities across military and intelligence entities is only one of many related components in long-term defense planning. Decision makers should thus give thought to how the organizing impacts the broader strategic, tactical, and operational prioritization between intelligence and military objectives. When is maneuvering in cyberspace for intelligence purposes vis-a-vis military cyberspace operations mutually exclusive, reinforcing, and supporting? What are the limitations, opportunities, and tensions? How to make sure that increased collaboration and sharing of (human, technical, and economic) resources across military and intelligence entities create the desired effectiveness, synergy, and flexibility? How to make sure that priorities and decisions share the same goals?

Third, it is paramount to strengthen the awareness of how organizational divergences might hamper collaboration at the level of intelligence sharing, EU cybersecurity governance, and NATO cyber operations. This is not least important in the context of a new EU Strategic Compass that aims at expanding the union’s “capacity to tackle cyber threats, disinformation and foreign interference” (European Union External Action Service 2022, 7), and a new Strategic Concept for NATO stating that “cyberspace is contested at all times. Malign actors seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities” (NATO 2022 Strategic Concept, 5). While there seems to be agreement on the cyber threat landscape, the model of future engagement and collaboration between NATO and the EU is in need of additional clarification.

Fourth, the findings shed additional light on our understanding of how the blurring of boundaries between war and peace, military and civilian, and internal and external security, identified in security studies in the past decades, looks in the cyber domain (Christensen and Liebetrau 2019). While we have seen a proliferation of military cyber commands among NATO members in the past decade (Pernik 2020; Smeets 2019), the military involvement in cyber affairs is often justified with reference to the permanence of cyberwar on the political side. This has arguably led to ‘overly militarized approaches to cyber security’ (Burton and Christou 2021, 1732). Giving more thought to the organizing of offensive cyber capabilities - and its entanglements - would equip scholars and decision makers to better engage the discussion of when and whether a warfare, competition, or intelligence framework is the most suitable for cyberspace.

Disclosure statement
No potential conflict of interest was reported by the author(s).
Notes

1. A Russian-led supply chain attack compromising the widely used SolarWinds software. It provided the Russian intelligence service with the ability to infect SolarWind users. The attack meant ‘that Russian intelligence had potential access to as many as 18,000 SolarWinds customers. They ultimately broke into fewer than 100 choice networks— including those of Fortune 500 companies like Microsoft and the US Justice Department, State Department, and NASA’ (Newman 2021). According to Microsoft President Brad Smith, ‘the largest and most sophisticated attack the world has ever seen’ (Villarreal 2021).

2. A Chinese-led hacking spree exploiting vulnerabilities in Microsoft’s Exchange Server to gain access to more than 30,000 victims in the US alone (Conger and Frenkel 2021).

3. A ransomware attack allegedly carried out by Russian criminals. The attack made Colonial Pipeline – a company Controlling almost half of the gasoline, jet fuel and diesel flowing along the East Coast of the US – turn off the spigot (David and Perlroth 2021).

4. I recognize the scholarly literature on international law and the use of cyber force, but it falls outside the scope of this article to deal with it in length (see e.g. Delerue (2020); Haataja (2019); Roscini (2014) and Schmitt (2017)).

5. See the website of the Dutch Ministry of Defence: https://english.defensie.nl/topics/cyber-security/cyber-command

6. ‘The Dutch intelligence services is known for having disrupted the Russian hacker groups Cozy Bear and Fance Bear (Hogeveen 2018) as well as the Russian military intelligence service Gru (Crerar, Henley, and Wintour 2018). Some of this work is undertaken in collaboration with the civilian General Intelligence and Security Service (AIVD) in the Joint SIGINT Cyber Unit (JSCU).’ (Liebetrau 2022, 16).

7. The Joint Sigint and Cyber Unit (JSCU). JSCU is a collaboration between the two Dutch intelligence and security services – the MIVD and the General Intelligence and Security Service (AIVD). The JSCU forms the cornerstone of the Dutch defense against advanced state-sponsored cyberattacks (advanced persistent threats) targeting ministries, infrastructure providers, and companies. The primary tasks of the unit are the collection of signal intelligence and the delivery of intelligence through cyber operations.

8. The highest-ranking civil servant in the Dutch Ministry of Defence. For the JSCU it is shared with the corresponding official of the Ministry of Justice and Security.

9. These operations are based on 2017 Intelligence and Security Services Act and are not conducted as military operations.


11. The French defence procurement and technology agency (DGA) is responsible for project management, development, and purchase of weapon systems for the French military.

ORCID

Tobias Liebetrau http://orcid.org/0000-0001-6996-9328

References


Forsvarsdepartementet 2014. *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner*.

Hogeveen, Bart. 2018. A Rare Insight into Cyber Espionage: Dutch Intelligence and Two Russian Bears. Australian Strategic Policy Institute.
Ministère des Armées 2019b. Éléments publics de doctrine militaire de lutte informatique offensive.
Ministère des Armées 2021. Éléments publics de doctrine militaire de lutte informatique d’influence.


