2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

The Global Spread of Cyber Forces, 2000–2018

Jason Blessing
DAAD Post-Doctoral Fellow[1]
Foreign Policy Institute
Johns Hopkins School of Advanced International Studies
Washington, DC, United States
jblessing@jhu.edu

Abstract: Although militaries have been building cyber capabilities since the late 1980s, formalized military organizations for these capabilities have only recently emerged. These cyber forces—active-duty military organizations that possess the capability and authority to direct and control cyberspace operations for strategic ends—have spread rapidly across the international system since the first few years of the 21st century. This article catalogues the development of cyber forces across the globe and assesses the various force structures. Existing research has largely been confined to examinations of cyber forces in North Atlantic Treaty Organization (NATO) member states. This article provides a broader view of global developments by introducing new data on the worldwide spread of cyber forces from 2000 to 2018. It also offers a typology for assessing cyber force structure based on both organizational model (branch, service, or joint model) and the scale of command (subordinated, sub-unified, or unified). As a result, this article identifies nine distinct cyber force structures. Empirical analysis reveals that 61 United Nations member states had created a cyber force by 2018. Contrary to conventional expectations, this analysis shows increasing variation in cyber force structure over time; no dominant organizational model or force structure has emerged.[2]

Keywords: *cyber forces, cyber force structure, military organizations, cyberspace operations*

[1] Position funded by the German Academic Exchange Service (DAAD).

[2] This article was supported by a U.S. Institute of Peace-Minerva Peace Scholar Award from USIP. The views expressed in this article are those of the author and do not necessarily reflect the views of the U.S. Institute of Peace.

1. INTRODUCTION

Militaries have been building cyber capabilities since the late 1980s (Wiener 2016); however, formalized military organizations for these capabilities have only recently emerged. The United States Cyber Command, created in 2010 and elevated to an independent unified combatant command in 2017, stands as an obvious example. A variety of other states have also established their own "cyber commands," including South Korea in 2010; Colombia in 2011; the United Kingdom, Turkey, and Spain in 2013; and the Netherlands and Ecuador in 2014 (Keck 2014; *Dialogo* 2013; Osula 2015; Seker and Tolga 2018; Cendoya 2016; Kaska 2015; Directorate of Social Communication of the Joint Command of the Armed Forces of Ecuador 2015).

To date, systematic research on cyber forces[3] has focused more on evaluating organizational maturity than on assessing variations in force structure (for example, see Robinson et al. 2013; Smeets 2019). Extant studies of force structure have tended to examine individual cases like the United States, Russia, China, and North Korea (Nielsen 2016; Lilly and Cheravitch 2020; Costello and McReynolds 2018; Kong et al. 2019). Research in a comparative context has been rare (Gorwa and Smeets 2019). As a notable exception, Pernik (2018) identifies three types of cyber forces: divisions under logistical branches; standalone combat services; and independent combatant commands/branches. Although Pernik (2018) is the first study to explicitly compare organizational arrangements, it captures only a fraction of the possible variation in force structure. Its scope is also limited to five European states, with Finland the only non-NATO state examined.

The lack of extensive comparative research on cyber force structure is problematic for at least two reasons. First, many expectations regarding military organizations are rooted in assumptions about the competitive or normative emulation of dominant paradigms (Resende-Santos 2007; DiMaggio and Powell 1983). For example, as militaries grappled with air power, an independent air force gradually emerged as the dominant organizational paradigm over other alternatives like separate air wings for each service (Hasik 2016). Such expectations leave scholars and practitioners without an appropriate terminology for understanding cyber forces. Indeed, referring to all institutional arrangements as "cyber commands" masks important variation in the scope, roles, and responsibilities in cyberspace. Second, force structures and the organizational origins of cyber forces can shape behavior and the tradeoff between exploitation and disruption. For instance, cyber forces originating in combat services may be more predisposed to take overt military action in cyberspace than those emerging from military intelligence, which may prefer information collection and covert operations (Schneider 2019, 115–120).

[3] Some works use the terms "military cyber organization" or "cyber command." This paper uses "cyber force," since "cyber force structure" is more concise than "military cyber organization force structure" and more precise than "cyber command structure."

This article builds on the works cited above and previously unpublished work (Blessing 2020b) to offer a broader perspective by cataloging the global development of cyber forces. Accordingly, the paper introduces a new database on cyber force structures and examines trends across states both in and outside the North Atlantic Treaty Organization. This paper also advances a novel typology of force structure that provides a foundation for addressing questions related to organizational structure and strategic behavior in cyberspace.

This paper proceeds in five sections. Section 2 defines cyber forces, while Section 3 provides a novel framework for distinguishing cyber forces structures based on organizational model (branch, service, joint) and scale of command (subordinated, sub-unified, unified). Section 4 presents a new database on the global spread of cyber forces from 2000 to 2018. Analysis reveals that 61 United Nations member states had created a cyber force by 2018. The data also show increasing variation in force structure over time; no dominant cyber force structure has emerged. Section 5 explores the implications for NATO, while Section 6 concludes by summarizing and considering future research.

2. DEFINING CYBER FORCES

Existing works describe cyber forces as a kind of military organization with some degree of authority over cyber operations. Pernik (2018, 2–3) states that the term "cyber force" "generally denotes a standalone structure, branch, or service of the armed forces that directs and controls the three main categories of cyberspace operations [defense, exploitation, attack]." Similarly, Smeets (2019, 165) defines a cyber force 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."

Yet not all cyber forces will have the mandate over the full spectrum of operations (as advanced by Pernik) or the full capability to undertake offensive operations (as laid out by Smeets). Moreover, these definitions are generally agnostic as to the strategic ends pursued by cyber forces. A key problem for distinguishing force structures, then, is determining which organizations are excluded.

This article defines cyber forces as active-duty military organizations with the capability and authority to direct and control strategic cyberspace operations to influence strategic diplomatic and/or military interactions (on cyberspace operations and strategic interactions, see Valeriano and Maness 2015). Cyberspace operations can include defense to prevent the compromise of the integrity, confidentiality, or availability of information on computers, the computers themselves, or networks; exploitation to collect information from an adversary's computers and networks that fall short of disrupting or destroying information; and attacks to disrupt, deny, degrade, or destroy information on computers or the computers or networks themselves. Espionage and theft constitute attacks when information or systems are destroyed (Healey 2013, 279–280).

This definition excludes three types of organizations with similar missions. The first is civilian intelligence agencies like the U.S. National Security Agency. Despite potentially significant overlaps in operations, the primary purposes of civilian agencies and cyber forces are fundamentally different. Aside from falling outside military chains of command, civilian intelligence agencies are largely focused on information collection. While cyber forces can and do collect information, intelligence-gathering is generally in service of and subordinated to gaining strategic advantage.

Second, purely reservist components—like Estonia's Cyber Defense Unit and Latvia's Cyber Defense Unit (Gramaglia et al. 2013; Gelzis 2014)—are excluded. Although reservists can provide several benefits (Miller et al. 2013; Baezner 2020), reservist units cannot maintain full-time authority over cyberspace operations. Reservist operation is conditional on legal activation (Brenner and Clarke 2011), and many governments maintain restrictions on using reserve funds for operational missions. Reservist units are also highly fluid: they consist of volunteers serving for only limited periods. This fluidity can compromise the up-to-date knowledge of operations, scalability, and interoperability required of active-duty organizations (Applegate 2012; Curley 2018). Overcoming such challenges would require substantial volunteering past minimum requirements, an assumption unlikely to hold across militaries.

Finally, military computer emergency readiness teams (MilCERTs), incident response teams (MilCIRTs), and incident response centers (MilCIRCs) are excluded. These organizations—like the Jordanian Armed Forces' MilCERT and Moldovan Armed Forces' MilCIRC (North Atlantic Treaty Organization 2017; de Albuquerque and Hedenskog 2016)—look for and patch military and/or defense network vulnerabilities, develop plans to deal with network outages and malicious attacks, and coordinate responses (Healey 2013, 279). They work defensively at the tactical level to ensure network operability but do not seek to integrate capabilities on larger operational or strategic scales. While they can be under the control of/report to cyber forces, they do not constitute cyber forces.

3. A FRAMEWORK FOR CYBER FORCE STRUCTURE

Like traditional force structure, cyber force structure is crucial for understanding how militaries translate material and human strengths into power on the battlefield. Force structure conventionally refers to the number and types of combat units a military can generate and sustain. It can be defined in several ways: the composition and structure of organizations; unit functions; capabilities; costs of operation; or some combination of these factors (Congressional Budget Office 2016). Unfortunately, much of these data for cyber forces—like personnel costs, operating costs, and capability acquisitions—are either inconsistently documented or remain classified.

This paper proposes two criteria for categorizing cyber force structures: organizational model and scale of command. These dimensions provide important insight into cyber forces' internal organization and how they relate to command structures across the military's combat and combat support subsystems (on militaries as organizations with subsystems, see Farrell 1996). Organizational model helps define combat service membership, internal divisions of labor, and how the cyber force relates to other military components (Augier et al. 2015). Scale of command illuminates the delegation of authority and responsibilities in military hierarchies. Thus it helps assess how operations are coordinated and/or integrated across other mission areas (Brooks 2006, 405–407).

There are three potential organizational models: a branch, service, or joint model. Under a *branch* model, authority for cyberspace operations rests primarily in logistical branches, military intelligence agencies, or signals corps within the combat support subsystem. While combat services can provide personnel for staffing, branch model forces fall outside service department chains of command.[4] Accordingly, a branch model arranges personnel along functional lines—specific expertise, tools, or missions—and not service-based ones. Cyber forces are organized according to a *service* model when a single combat service—domain-based (army, navy, air force) or functional (such as rocket forces, marines, or other standalone services)—retains primary authority for cyberspace operations. In these instances, a cyber force is staffed only by personnel from the combat service to which it reports. Like a branch model, service model personnel are generally grouped according to functional expertise in units or component commands. A *joint* model entails the shared distribution of authority across two or more combat services. Under this model, combat services are force providers—cyber forces rely primarily on the services for staffing and funding. Staffing generally occurs on a short-term, rotational basis. In other words, combat services provide personnel for specific periods before they are recalled to service-based assignments and replaced in the cyber force with other service personnel.

[4] While combat support elements are present within combat subsystems, combat is the overarching functional role for that subsystem.

A joint model thus serves to facilitate coordination among service components. Therefore, service membership is the primary organizing principle within a joint model; functional expertise is a secondary principle.

Cyber forces can also be classified by subordinated, sub-unified, or unified commands. *Subordinated* cyber forces appear when existing commands incorporate cyberspace operations to support ongoing missions and enhance effectiveness without disrupting status quos (on military adaptation, see Farrell 2010). *Sub-unified* force structures consist of specialized sub-organizations that treat cyber operations as an independent mission. These can result from reconfigurations of personnel and capabilities within subsystems to implement novel operational concepts or technologies. *Unified* forces institutionalize "new ways of war" (Rosen 1991) related to the cyber domain via a new branch, service, or combatant command. They can emerge from military-wide reorganizations that disrupt relationships and interdependencies. Unified forces have no parent organization and report directly to chiefs/ministers/secretaries of defense. Sub-unified forces report to existing unified commands; subordinated forces report to sub-unified (and, in rare cases, unified) parent commands.

These two dimensions of force structure have important implications for the functioning and behavior of cyber forces. For example, all else held equal, unified cyber forces with greater scales of command are likely to be better resourced, better staffed, and better positioned to compete for additional resources than sub-unified or subordinated forces. Scale of command also provides a proxy for the development of and degree to which cyber capabilities are considered an independent military tool. The branch, service, and joint models give additional insight into behavior. For instance, because a joint model incorporates multiple service elements, it can facilitate the development of doctrine for multi-domain operations. Yet a joint model must also grapple with service prerogatives and parochialism that can hamper effectiveness. Inter-service competition similarly affects service model cyber forces. And while service models may be able to better develop cyber personnel (through specialized service academy training and new career paths), they risk losing mission independence to existing service priorities. Branch model forces also risk subordination to combat service missions that prevents the development of independent capabilities.

Table I summarizes the nine cyber force structures produced by these criteria. A brief description of the nine force structures with illustrative examples accompanies Table I.

TABLE I: A TYPOLOGY OF CYBER FORCE STRUCTURES

	Scale of Command		
Organizational Model	**Subordinated**	**Sub-Unified**	**Unified**
Branch	(1) Subordinated Branch	(4) Sub-Unified Branch	(7) Unified Branch
Service	(2) Subordinated Service	(5) Sub-Unified Service	(8) Unified Service
Joint	(3) Subordinated Joint	(6) Sub-Unified Joint	(9) Unified Joint

(1) Subordinated Branch: non-service communications divisions, signals intelligence units, or military intelligence agencies that integrate cyberspace operations into existing command structures. Examples include Israel's Unit 8200, an electronics intelligence unit under the Directorate of Military Intelligence; and Estonia's Strategic Communications Center, a unit under the Support and Signals Battalion until 2018 (Lewis and Neuneck 2013; Osula 2015a).

(2) Subordinated Service: one combat service co-opts the cyber mission into existing electronic warfare, signals, or communications units; no other services have the capability or mandate to conduct cyberspace operations. The Danish Army's 3rd Electronic Warfare Company (2009–2012) and the Philippine Army's Signals Corps (operational in 2016) are examples of service units with primary responsibilities for cyberspace operations (International Institute for Strategic Studies 2013; Felongco 2016).

(3) Subordinated Joint: primarily temporary, issue- or mission-driven task forces or units that coordinate the cyber mission across two or more combat services. A Subordinated Joint force structure does not include major service-level commands as components. Examples include a variety of joint task forces in the United States (2001–2010)[5] and France's Cyber Defense Cell (2011–2015; see Brangetto 2015).

(4) Sub-Unified Branch: new cyber divisions or directorates under military intelligence agencies, communications/information systems agencies, or joint staff support directorates. Examples include the Finnish Cyber Defense Division (2015–present) and the Cyber Security Operations Center under the Belgian Military Intelligence Service (Pernik 2018; Lasoen 2019).

[5] Joint Task Force – Computer Network Operations (2001–2004), Joint Task Force – Global Network Operations (2004), and Joint Functional Component Command – Network Warfare (2005–2010). U.S. Cyber Command, "U.S. Cyber Command History," n.d., https://www.cybercom.mil/About/History/.

(5) Sub-Unified Service: major commands within a combat service for conducting cyberspace operations that are on par with existing service commands and missions. Although it can be staffed with personnel from other services, this structure is subordinated to only one service. Examples include Nigeria's Cyber Warfare Command (operational in 2018), which consolidates the Army's efforts into a new service command; and Brazil's Cyber Defense Command (2017–present), which incorporates personnel from the Army, Navy, and Air Force but is under the sole authority of the Army (Moury 2017; Omonobi-Abuja 2018).

(6) Sub-Unified Joint: structure that reports to an existing joint unified combatant command, significantly expanding that parent command's scope of operations. Unlike subordinated structures, Sub-Unified Joint structures are necessarily comprised of major commands from at least two services. United States Cyber Command under U.S. Strategic Command (2010–2017) and Italy's Joint Command for Cyberspace Operations under the Joint C4 Defense Command (operational in 2017) fall in this category (Italian Ministry of Defence 2018).

(7) Unified Branch: independent non-combat military branches that hold special armament or equipment to conduct missions in the cyber domain. Examples include Estonia's Cyber Command (2018–present) and Norway's Cyber Defense Force (2012–present) (Estonian Defence Forces, 2018; Ministry of Defense of Norway 2012).

(8) Unified Service structures are cyber-specific combat services (with military departments) that receive the same hierarchical standing as other domain-based services (armies, navies, and air forces). Only China's Strategic Support Force (2016–present) and Germany's Cyber and Information Domain Service (2017–present) utilize this force structure (International Institute for Strategic Studies 2019; Pernik 2018).

(9) Unified Joint: unified combatant commands for cyberspace comprised of at least two service-level component commands. These independent commands report directly to the top defense official. Examples include U.S. Cyber Command (2017–present) and the Netherlands' Defense Cyber Command (2018–present).

4. CYBER FORCES IN THE WORLD, 2000–2018

To assess the global spread of cyber forces, this article uses a custom-created database introduced in Blessing (2020b): the Dataset on Cyber Force Structures (DCFS). This new database catalogues cyber force structures for the 172 United Nations (UN) members with an active military force from 2000 to 2018. An active military force is a necessary precondition: there can be no cyber force without an active military. Accordingly, the DCFS excludes the 21 UN member states that do not maintain active military forces.[6]

The dataset utilizes five types of sources: government publications; reports from think tanks or international organizations; peer-reviewed academic works; articles from international and regional news outlets; and interviews with former policymakers, military officials, industry members, and subject matter experts. Inclusion in the author-coded dataset requires satisfying the following basic criteria:

- A government source identifies an organization responsible for cyberspace operations. Government sources are corroborated by two other resources. Where government sources are unavailable or lack detail, information is derived from three different categories of resources.

- When multiple organizations are responsible for cyberspace operations, cyber forces are coded based on the military hierarchy: organizations higher in the chain of command with operational responsibilities are designated as the primary cyber force. For example, Denmark's cyber force in 2009–2012 was the Army 3rd Electronic Warfare Company; however, because the Offensive Cyber Warfare Unit (established 2012) under the Defense Intelligence Service had fewer links in the chain of command to the joint Defense Command and Minister of Defense, it replaced the Army's unit as the primary cyber force despite the latter's continued operation.

- Organizational model is based on subsystem and the number of combat services providing personnel. Subsystem is coded on the reporting structures of parent commands. For example, Germany's Department of Information and Computer Network Operations, formerly under the Joint Support Service's Strategic Reconnaissance Command, is coded as combat support. Where no parent organization exists (i.e., for unified commands), subsystem rests on whether the force falls under service chains of command or is a non-

[6] Because the database was originally presented as part of doctoral dissertation work in Blessing (2020b), the first round of data collection efforts, covering the period between January 2000 and December 2018, concluded in 2019. As such, the data below do not reflect the most up-to-date force structures for each country. A second round of data collection and coding, which will update the DCFS for the 2019–2021 period, is currently underway and is scheduled to be completed in early 2022.

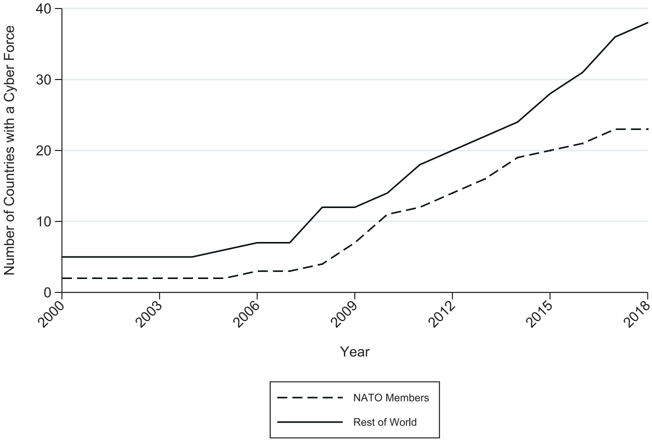
service force. Cyber forces in combat support subsystems are branch model. Cyber forces in combat subsystems are either service model (one service) or joint model (two or more services). Joint models occur when services are formally linked by a supra-command or maintain independent cyber forces. When multiple services have cyber forces that report to only one service, a service model is coded.

- Scale of command is determined by immediate parent organizations and reporting structures. Unified commands have no parent organizations and report to chiefs/ministers/secretaries of defense. Unified commands are joint combatant commands, independent combat services, or independent branch commands. Sub-unified commands report to unified commands; they encompass joint component commands, combat service major commands, and major commands reporting to an independent branch. Subordinated commands report to sub-unified commands (and, in rare cases, unified commands); they appear as task forces, joint units under component or combatant commands, units in a service-level major command, or functional branch units.

Each observation in the dataset thus contains the following descriptive information: country name; the name of the organization with authority over cyberspace operations as it appears in the military hierarchy; an operational start date (month/year) indicating initial operating capability; an operational end date (month/year) indicating when the organization was disbanded based on expansion, reorganization, and consolidation, or replacement with new initiatives that change the military hierarchy; the parent command to which the organization directly reports; the organization's location in either the combat or combat support subsystem; and the number of combat services staffing the organization.

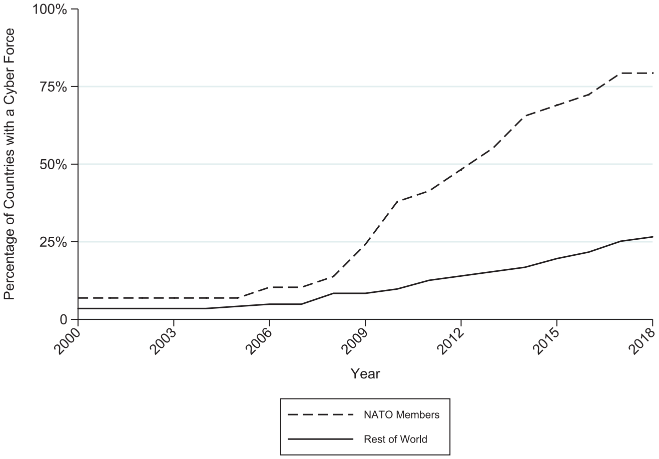
Figures 1 and 2 chart the development of cyber forces within NATO countries and in the rest of the world between 2000 and 2018. Figure 1 shows the overall counts; Figure 2 provides the percentage of NATO and non-NATO countries with a cyber force. A summary of cyber force structures for both NATO and non-NATO countries is provided in the Appendix for the year 2018, the latest year for which the dataset has been updated.

FIGURE 1: THE TOTAL GROWTH OF CYBER FORCES IN AND OUTSIDE NATO



Source: Dataset on Cyber Force Structures

FIGURE 2: THE PERCENTAGE OF STATES WITH A CYBER FORCE IN AND OUTSIDE NATO



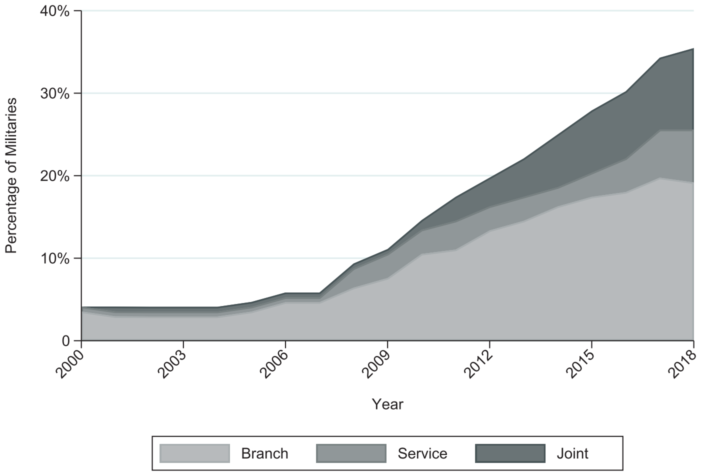
Source: Dataset on Cyber Force Structures

In 2000–2004, only seven countries maintained cyber forces: the United States, Russia, China, Israel, North Korea, Greece, and Thailand each had cyber forces prior to 2000. Worth noting is the consistent increase in cyber forces post-2007. In 2007, there were a total of 10 cyber forces: three in NATO and seven outside NATO. By 2018, there were 61 cyber forces (35.5 percent of militaries) across the world—an average global growth rate of 2.7 percent (four to five new cyber forces) per year since 2007. NATO members accounted for 23 of these 61 forces (Blessing 2020a).

As Figure 1 indicates, non-NATO cyber forces outnumbered NATO-member cyber forces between 2000 and 2018. This trend will inevitably continue, as the number of non-NATO countries is far greater than the number of NATO members. However, Figure 2 provides additional context: cyber forces have emerged at a much faster rate among NATO members than among non-NATO countries. This is particularly clear from 2008 to 2018. Less than 25 percent of NATO countries had a cyber force in 2008. By 2018, nearly 80 percent of NATO countries had developed a cyber force. Conversely, not until after 2017 were there cyber forces in more than 25 percent of non-NATO countries. Thus NATO members have created cyber forces more quickly than the rest of the world; the data suggest that the alliance may be playing a facilitating role. Although the growth of cyber forces in non-NATO states will eventually outpace that of the remaining NATO members over time, NATO countries have led the way in developing military organizations for cyberspace.

Figure 3 shows the global growth of the branch, service, and joint models over time. Significantly, as the number of cyber forces has increased, so has the variation in organizational model. Until 2008, roughly 75 percent of cyber forces utilized the branch model; by 2018, approximately 55 percent of cyber forces used the branch model (a 20 percent drop). While the utilization of the joint model has grown over time, it only accounts for just over 25 percent of the variation by 2018. What Figure 3 indicates is that, although most cyber forces have been structured according to a branch model, the relative prevalence of the branch model has decreased over time. This increasing variation over time runs counter to expectations regarding the emergence of a dominant organizational model.

FIGURE 3: THE WORLDWIDE GROWTH OF CYBER FORCES BY ORGANIZATIONAL MODEL



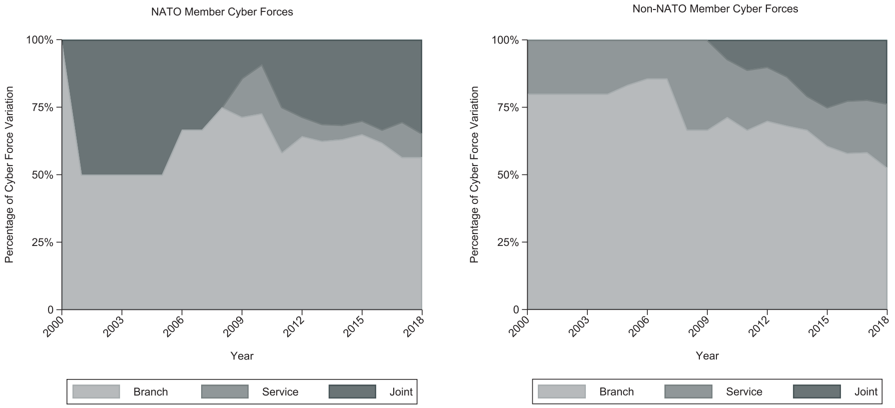
Source: Dataset on Cyber Force Structures

Figure 4 breaks down the variation in organizational model for the cyber forces of NATO members and non-NATO states (2000–2018), while Figure 5 shows the proportion of subordinated, sub-unified, and unified commands from 2009 to 2018 for cyber forces in and outside NATO.

As with Figure 3, the distributions of organizational models in Figure 4 indicate increasing variation over time across cyber forces in both NATO member states (left) and non-NATO states (right). While the branch model has accounted for most cyber force structures, its usage has declined in both groups over time (although somewhat more consistently in non-NATO states). Notably, non-NATO states have opted for the service model at a higher rate than NATO members, while NATO members have used the joint model more extensively than the service model. However, as of 2018, there was no dominant organizational model.

There are several takeaways from Figure 5. First, sub-unified commands only emerge in 2010; the three to appear in 2010 were South Korea's Cyber Command (sub-unified branch), U.S. Cyber Command (sub-unified joint), and Iran's Cyber Defense Command (sub-unified joint). Second, unified commands appear only after 2012 (Norway's Cyber Defense Force, a unified branch, was the first). Third, subordinated commands have been the most prevalent command in non-NATO states. However, by 2018 only half of non-NATO cyber forces were a subordinated command; less than 20 percent had implemented a unified command. Conversely, nearly 40 percent of NATO cyber forces were a unified command by 2018, and less than 20 percent were a subordinated command. On average, a greater proportion of NATO member cyber forces were able to develop into sub-unified and unified commands than non-NATO cyber forces.

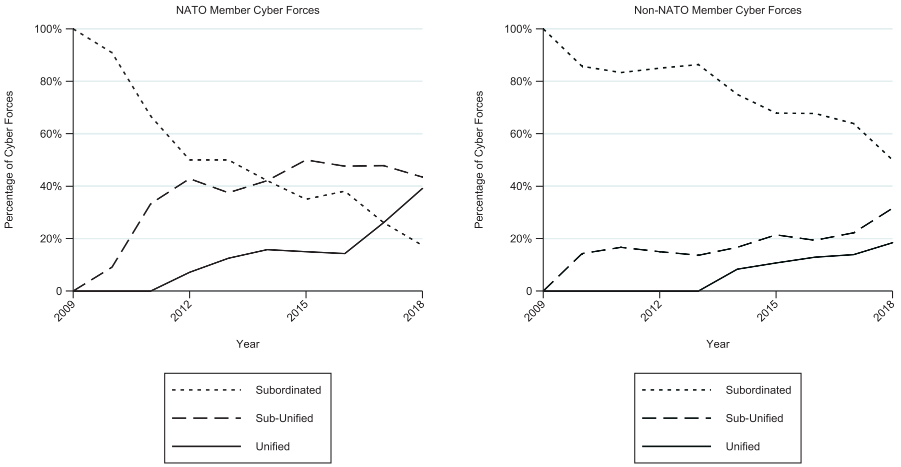
FIGURE 4: MODEL DISTRIBUTION ACROSS CYBER FORCES



Source: Dataset on Cyber Force Structures

Source: Dataset on Cyber Force Structures

FIGURE 5: COMMAND DEVELOPMENTS IN AND OUTSIDE NATO



Source: Dataset on Cyber Force Structures

Source: Dataset on Cyber Force Structures

Collectively, Figures 2 through 4 indicate that a subordinated branch has been the most prevalent cyber force structure for both NATO members and non-NATO states. Concluding that this is the predominant force structure, however, is misleading. Each of these figures shows increasing variation over time in both organizational model and scale of command. As new cyber forces were created and existing ones elevated within militaries, there was a decline in the use of the subordinated branch structure relative to other force structures. With the move away from subordinated branches towards unified force structures, can unified cyber forces provide insight into an emerging dominant force structure?

Even across unified cyber forces, the data show variation. Table II looks at all unified cyber force structures in 2018. Across NATO member states as well as rest of the world, unified joint force structures (nine total) were only slightly favored over unified branch (five total) or unified service (two total) arrangements. With only 16 total cyber forces at the unified command level, the unified joint cyber force structure is by no means the predominant paradigm. Evidence thus suggests that, instead of conforming to a single cyber force structure, states have tailored the creation and implementation of cyber forces to their own respective circumstances.

TABLE II: UNIFIED CYBER FORCE STRUCTURES, 2018

	NATO Members	Rest of World	Total
Unified Branch	3	2	5
Unified Service	1	1	2
Unified Joint	5	4	9
Total	9	7	16

Given the variation in cyber force structure across the globe—and between NATO-member states and non-NATO states—what factors can explain force structure choices? Arguably, joint models require greater resource levels and redundant capabilities across combat services than do service or branch models. Likewise, scales of command are likely to be influenced by military spending levels, the size of the workforce, and strategic development. This could be one reason why the joint model and unified commands are somewhat more prevalent across NATO countries: the world's largest economies are disproportionally represented in NATO compared to the rest of the world (World Bank 2018). Although outside the scope of this article, examining the relative influence of these factors on force structure selection and change over time represents fertile ground for future research.

5. IMPLICATIONS FOR NATO

While the force structure data presented above shed light on the cyber force initiatives across NATO's member countries, the individual force structure decisions of states also affect how NATO itself approaches the cyber domain. This paper's findings carry three main implications for NATO.

First and foremost, the rapid increase in the number of NATO members with cyber forces necessitates the development of robust frameworks for integrating sovereign cyber effects into NATO operations (North Atlantic Treaty Organization 2018). The goal of these efforts should be for the alliance to achieve greater effectiveness in cyberspace, particularly as the Cyber Operations Centre relies on personnel from member states with varying capability levels. Additionally, the alliance must start to grapple with the implications of out-of-network operations conducted by members on other allies' networks (Smeets 2019b). At the same time, NATO must account for the inevitable increase in military footprints in cyberspace emerging outside the alliance. The alliance has been at the forefront in setting the international agenda for cyber issues (Brent 2019). As more states develop cyber forces and existing forces become more mature, NATO and its members are presented with new opportunities to collaborate with non-NATO states.

In this regard, one fruitful way forward for the alliance is to strengthen existing partnerships with non-NATO states and entities. Similar to the 2016 Joint Declaration on NATO-EU Cooperation, the alliance should look to build on its relationships cultivated through the Partnership Interoperability Initiative launched in 2014 (North Atlantic Treaty Organization 2020). More specifically, the alliance could benefit from new initiatives with Enhanced Opportunity Partners like Sweden and Finland, both of which have participated in NATO cyber defense exercises; the latter has also signed the 2017 Political Framework Arrangement on cyber defense cooperation with NATO. Additionally, the alliance could seek to create stronger ties with Australia, a country that has been explicit about its pursuit of offensive capabilities and norm-building in cyberspace (Uren 2018). Other Interoperability Platform Partners like Austria, Japan, South Korea, and Switzerland also offer opportunities to build bridges with established cyber forces. With a broader set of partners, NATO can seek to exchange concepts and develop best practices, test these in exercises, and draw lessons for capability development.

Second, this paper's conceptual framework is important for NATO's net assessment efforts. Force structure is a key aspect of net assessment; however, many elements of traditional force structure become problematic when applied to cyber forces. Several examples illuminate the necessity of this paper's typology for net assessment. Unlike unit functions in other domains,[7] operational functions in the cyber domain can be nearly indistinguishable. Both attacking a network and defending one's own can rely on intrusions into an adversary's networks for intelligence collection. Network exploitation, defense, and attack also use similar tools and techniques (Buchanan 2017, 15–96).

Moreover, instead of tangible weapons systems (missiles, tanks, submarines, etc.) that have multiple-use ability and are quantifiable, "cyberweapons" are comprised of largely digital, transitory elements that have only a temporary ability to access and attack computer networks and systems (Smeets 2018). Capabilities also rapidly diffuse to others: after detecting and patching vulnerabilities after an attack, adversaries can modify and redeploy a capability against the original attacker (Buchanan 2016). Finally, while conventional personnel can be assessed according to the number of direct and indirect military personnel per unit, cyber force personnel complicate net assessments. While total personnel can be quantified, there is no clear distinction between direct "combat" and indirect "support" personnel in the cyber domain. Indirect roles—like signals intelligence—are at the heart of operations for cyber forces' direct personnel.

[7] Such as armored combat and infantry in the land domain; aircraft carriers and amphibious ships in the maritime domain; bombers and airlift in the air domain; and special operations across domains.

For these reasons, this paper's typology provides the alliance an alternative way to assess force structure; this is particularly important should NATO establish an Office of Net Assessment, as recommended by the NATO 2030 Reflection Group (NATO Reflection Group 2020, 24).

Third, and more broadly, this paper highlights the need for NATO to develop a strategic political framework for coordinating military cyber defense for the alliance and its members. The 2010 Strategic Concept gave relatively little attention to military cyber defense; in fact, the document only uses the word "cyber" five times (North Atlantic Treaty Organization 2010). The data presented in this article indicate that conditions are ripe for integrating cyber defense into the alliance's future strategic concepts. NATO's 2016 recognition of cyberspace as an operational domain, the Cyber Defense Pledge among members, and the establishment of the Cyber Operations Centre have been important milestones. However, the alliance should better define how cyberspace relates to existing core tasks of collective defense, crisis management, and cooperative security. Integrating cyber capabilities into collective defense efforts looms particularly large. For example, the disparity in force structures among members highlights the need to develop a strategy for multi-domain operations, as different force structures are likely to emphasize different operational experiences and approaches to combining cyber capabilities with more traditional ones.

6. CONCLUSION

This paper has offered a comparative perspective of cyber forces and has introduced a new database that catalogues cyber forces from 2000 to 2018. It has also presented a new framework—based on both organizational model (branch, service, or joint model) and the scale of command (subordinated, sub-unified, or unified)—to identify nine unique cyber force structures.

Empirical analysis using this new dataset shows that in 2000, only seven UN-member states possessed cyber forces; 61 UN-member states had created a cyber force by 2018. The data portray consistent growth in the number of cyber forces worldwide; concomitantly, there has been increasing variation in cyber force structure over time. Contrary to conventional expectations, analysis shows that no dominant trends have emerged across either NATO member states or non-NATO states.

Future research can expand on this paper's analysis in several ways. This article did not address why a specific organizational model was chosen for cyber forces; future work can investigate the factors behind model selection for cyber forces. Additionally, future work can explore the facilitators and barriers behind decisions to change force structure. In this regard, case study research and process tracing political decision-making offer a fruitful way forward. Finally, research can assess how cyber forces change over the course of implementation efforts within militaries. This paper has offered only a static view of the development of cyber forces; a more dynamic view of cyber forces over time is necessary to understand the changing ways in which militaries approach the cyber domain.

REFERENCES

Albuquerque, Adriana Lins de, and Jakob Hedenskog. 2016. "Moldova: A Defence Sector Reform Assessment." FOI-R--4350--SE. Stockholm, Sweden: Swedish Defence Research Agency. https://www.foi.se/rest-api/report/FOI-R--4350--SE.

Applegate, Scott D. 2012. "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations." Fairfax, VA: Center for Secure Information Systems, George Mason University.

Augier, Mie, Thorbjorn Knudsen, and Robert M. McNab. 2015. "Advancing the Field of Organizations through the Study of Military Organizations." *Industrial and Corporate Change* 23 (6): 1417–44.

Baezner, Marie. 2020. "Study on the Use of Reserve Forces in Military Cybersecurity: A Comparative Study of Selected Countries." Zurich, Switzerland: Center for Security Studies, ETH Zurich. https://doi.org/10.3929/ethz-b-000413590.

Blessing, Jason. 2020a. "The Dataset on Cyber Force Structures." Unpublished raw data.

———. 2020b. "The Diffusion of Cyber Forces: Military Innovation and the Dynamic Implementation of Cyber Force Structure." Dissertation, Syracuse University, Syracuse, NY.

Brangetto, Pascal. 2015. "National Cyber Security Organisation: France." National Cyber Security Organisation. Tallinn, Estonia: NATO CCD COE. https://ccdcoe.org/library/publications/national-cyber-security-organisation-france/.

Brenner, Susan W., and Leo L. Clarke. 2011. "Conscription and Cyber Conflict: Legal Issues." In *2011 3rd International Conference on Cyber Conflict*, edited by C. Czosseck, E. Tyugu, and T. Wingfield, 1–12. Tallinn, Estonia: CCD COE Publications.

Brent, Laura. 2019. "NATO's Role in Cyberspace." *NATO Review* (blog). February 12, 2019. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

Brooks, Risa. 2006. "An Autocracy at War: Explaining Military Effectiveness, 1967 and 1973." *Security Studies* 15 (3): 396–430.

Buchanan, Benjamin. 2016. "The Life Cycles of Cyber Threats." *Survival* 58 (1): 39–58.

———. 2017. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford: Oxford University Press.

Cendoya, Alexander. 2016. "National Cyber Security Organisation: Spain." National Cyber Security Organisation. Tallinn, Estonia: NATO CCD COE. https://ccdcoe.org/library/publications/national-cyber-security-organisation-spain/.

Congressional Budget Office. 2016. "The U.S. Military's Force Structure: A Primer." Washington, D.C.: Congress of the United States. https://apps.dtic.mil/dtic/tr/fulltext/u2/1014153.pdf.

Costello, John, and Joe McReynolds. 2018. “China’s Strategic Support Force: A Force for a New Era.” 13. China Strategic Perspectives. Washington, D.C.: Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, National Defense University. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

Curley, Gregg. 2018. “The Provision of Cyber Manpower: Creating a Virtual Reserve.” *MCU Journal* 9 (1): 191–217.

Dialogo. 2013. “Colombia Rises to the Cyber Challenge,” April 1, 2013. https://dialogo-americas.com/en/articles/colombia-rises-cyber-challenge.

DiMaggio, Paul J., and Walter W. Powell. 1983. “The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields.” *American Sociological Review* 48 (2): 147–60.

Directorate of Social Communication of the Joint Command of the Armed Forces of Ecuador. 2015. “Fuerzas Armadas realiza taller para defini Infraestructura critica” [Armed Forces conducts workshop to define Critical Infrastructure]. *Nota Periodistica No. 2015-04-20-01-DIR-C.S.*, April 20, 2015. https://www.ccffaa.mil.ec/2015/04/20/fuerzas-armadas-realiza-taller-para-definir-infraestructura-critica/.

Ertan, A., K. Floyd, P. Pernik, and T. Stevens, eds. 2020. “Cyber Threats and NATO 2030: Horizon Scanning and Analysis.” NATO CCD COE Publications. https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf.

Estonian Defence Forces. n.d. “Cyber Command.” http://www.mil.ee/en/landforces/Cyber-Command.

Farrell, Theo. 1996. “Figuring Out Fighting Organisations: The New Organisational Analysis in Strategic Studies.” *Journal of Strategic Studies* 19 (1): 122–35.

———. 2010. “Improving in War: Military Adaptation and the British in Helman Province, Afghanistan, 2006–2009.” *Journal of Strategic Studies* 33 (4): 567–594.

Felongco, Gilbert P. 2016. “Philippine Armed Forces Build Up Capability to Fight in Cyberspace.” *Gulf News*, November 23, 2016. https://gulfnews.com/world/asia/philippines/philippine-armed-forces-build-up-capability-to-fight-in-cyberspace-1.1934044.

Gelzis, Gederts. 2014. “Latvia Launches Cyber Defence Unit to Beef Up Online Security.” *Deutsche Welle*, March 4, 2014. https://www.dw.com/en/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936.

Gorwa, Robert, and Max Smeets. 2019. “Cyber Conflict in Political Science: A Review of Methods and Literature.” Working Paper Prepared for the 2019 ISA Annual Convention, Toronto, Canada,1–24. URL: 10.31235/osf.io/fc6sg.

Gramaglia, Matteo, Emmet Tuohy, and Piret Pernik. 2013. “Military Cyber Defense Structures of NATO Members: An Overview.” Background Paper. Tallinn, Estonia: International Centre for Defence and Security (RKK/ICDS). https://icds.ee/wp-content/uploads/2013/Military%20Cyber%20Defense%20Structures%20of%20NATO%20Members%20-%20An%20Overview.pdf.

Hasik, James. 2016. “Mimetic and Normative Isomorphism in the Establishment and Maintenance of Independent Air Forces.” *Defense & Security Analysis* 32 (3): 256–263.

Healey, Jason, ed. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington, VA: Cyber Conflict Studies Association.

International Institute for Strategic Studies. 2013. “Europe.” In *The Military Balance* 113: 89–198.

———. 2019. “Asia.” In *The Military Balance* 119: 222–319.

Italian Ministry of Defence. 2018. “Il Sottosegratario Tofalo visita il Comando C4 Difesa e il CIOC” [Undersecretary Tofalo visits the C4 Defense Command and the CIOC], August 1, 2018. https://www.difesa.it/Primo_Piano/Pagine/Il-Sottosegretario-Tofalo-visita-il-Comando-C4-Difesa-e-il-CIOC.aspx.

Kaska, Kadri. 2015. “National Cyber Security Organisation: The Netherlands.” National Cyber Security Organisation. Tallinn, Estonia: NATO CCD COE. https://ccdcoe.org/library/publications/national-cyber-security-organisation-the-netherlandskadri-kaskaactive-passive-cyber-defence-law-national-frameworks-policy-strategy-the-netherlands/.

Keck, Zachary. 2014. “South Korea Seeks Offensive Cyber Capabilities.” *The Diplomat*, October 11, 2014. https://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/.

Kong, Ji Young, Jong In Lim, and Kyoung Gon Kim. 2019. “The All-Purpose Sword: North Korea’s Cyber Operations and Strategies.” In *2019 11th International Conference on Cyber Conflict: Silent Battle*, edited by Tomas Minarik, S. Alatulu, M. Signoretti, I. Tolga, and G. Visky, 143–62. Tallinn, Estonia: CCD COE Publications.

Lasoen, Kenneth L. 2019. “Belgian Intelligence SIGINT Operations.” *International Journal of Intelligence and Counterintelligence* 32 (1): 1–29.

Lewis, James Andrew, and Gotz Neuneck. 2013. “The Cyber Index: International Security Trends and Realities.” New York and Geneva: United Nations Institute for Disarmament Research.

Lilly, Bilyana, and Joe Cheravitch. 2020. “The Past, Present, and Future of Russia’s Cyber Strategy and Forces.” In *20/20 Vision: The Next Decade*, edited by T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, and G. Visky, 129–155. Tallinn, Estonia: NATO CCD COE Publications.

Miller, Drew, Daniel B. Levine, and Stanley A. Horowitz. 2013. “A New Approach to Force-Mix Analysis: A Case Study Comparing Air Force Active and Reserve Forces Conducting Cyber Missions.” IDA Paper P-4986. Alexandria, VA: Institute for Defense Analyses.

Ministry of Defense of Norway. 2012. “Cyberforsvaret offisielt etablert i dag” [Cyber Defence Force officially established today]. September 18, 2012. https://www.regjeringen.no/no/dokumentarkiv/stoltenberg-ii/fd/Nyheter-og-pressemeldinger/Nyheter/2012/cyber/id699271/.

Moury, Taciana. 2017. “Brazilian Army Invests in Cyber Defense.” *Dialogo*, May 12, 2017. https://dialogo-americas.com/en/articles/brazilian-army-invests-cyber-defense.

NATO Reflection Group. 2020. “NATO 2030: United for a New Era.” https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

Nielsen, S. 2016. “The Role of the U.S. Military in Cyberspace.” *Journal of Information Warfare* 15 (2): 27–38.

North Atlantic Treaty Organization. 2010. “Active Engagement, Modern Defense: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.” https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

———. 2017. “NATO Supports Jordan’s National Cyber Defence Strategy,” July 19, 2017. https://www.nato.int/cps/en/natohq/news_146287.htm.

———. 2018. “Framework Mechanism for the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions.” North Atlantic Treaty Organization.

———. 2020. “Partnership Interoperability Initiative,” November 3, 2020. https://www.nato.int/cps/en/natohq/topics_132726.htm.

Omonobi-Abuja, Kingsley. 2018. “Nigerian Army’s Cyber Warfare Command Begins Operation.” *Vanguard*, August 29, 2018. https://www.vanguardngr.com/2018/08/nigerian-armys-cyber-warfare-command-begins-operation/.

Osula, Anna-Maria. 2015a. “National Cyber Security Organisation: Estonia.” National Cyber Security Organisation. Tallinn, Estonia: NATO CCD COE. https://ccdcoe.org/library/publications/national-cyber-security-organisation-estonia/.

———. 2015b. “National Cyber Security Organisation: United Kingdom.” National Cyber Security Organisation. Tallinn, Estonia: NATO CCD COE. https://ccdcoe.org/library/publications/national-cyber-security-organisation-united-kingdom/.

Pernik, Piret. 2018. “Preparing for Cyber Conflict: Case Studies of Cyber Command.” Tallinn, Estonia: International Centre for Defence and Security (RKK/ICDS).

Resende-Santos, Joao. 2007. *Neorealism, States, and the Modern Mass Army*. Cambridge: Cambridge University Press.

Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, and Pablo Rodriguez. 2013. “Stocktaking Study of Military Cyber Defence Capabilities in the European Union (MilCyberCAP): Unclassified Summary.” RAND Corporation.

Rosen, Stephen Peter. 1991. *Winning the Next War: Innovation and the Modern Military*. Ithaca and London: Cornell University Press.

Schneider, Jacquelyn. 2019. “Deterrence in and through Cyberspace.” In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Erik Gartzke and John Lindsay, 95–120. Oxford: Oxford University Press.

Seker, Esnar, and Ihsan Burak Tolga. 2018. “National Cyber Security Organisation: Turkey.” National Cyber Security Organisation. Tallinn, Estonia: NATO CCD COE. https://ccdcoe.org/library/publications/national-cyber-security-organisation-turkey/.

Smeets, Max. 2018. “A Matter of Time: On the Transitory Nature of Cyberweapons.” *Journal of Strategic Studies* 41 (1–2): 6–32.

———. 2019a. “NATO Members’ Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis.” In *11th International Conference on Cyber Conflict: Silent Battle*, edited by T. Minarik, S. Alatulu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky, 163–78. Tallinn, Estonia: NATO CCD COE Publications.

———. 2019b. “NATO Allies Need to Come to Terms With Offensive Cyber Operations.” *Lawfare* (blog). October 14, 2019. https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations.

Uren, Tom. 2018. “Australia’s Offensive Cyber Capability.” *The Strategist, Australian Strategic Policy Institute* (blog). April 10, 2018. https://www.aspistrategist.org.au/australias-offensive-cyber-capability/.

U.S. Cyber Command. n.d. “U.S. Cyber Command History.” Accessed July 13, 2019. https://www.cybercom.mil/About/History/.

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford and New York: Oxford University Press.

Wiener, Craig J. 2016. “Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation.” Doctoral dissertation, George Mason University, Fairfax, VA.

World Bank. 2018. “World Development Indicators.” Washington, D.C.: World Bank.

APPENDIX: NATO AND NON-NATO CYBER FORCE STRUCTURES, 2018

The data presented below describes cyber force structures for the year 2018, the most recent year for which the Dataset on Cyber Force Structures (DCFS) has been updated. Because the database was originally presented as part of doctoral dissertation work in Blessing (2020b), the first round of data collection efforts, covering the period between January 2000 and December 2018, concluded in 2019. As such, the data below do not reflect the most up-to-date force structures for each country. A second round of data collection and coding, which will update the DCFS for the 2019–2021 period, is currently underway and is scheduled to be completed in early 2022.

The organizational names provided below correspond to official national sources and have been translated into English.

TABLE III: CYBER FORCE STRUCTURE FOR NATO MEMBER STATES, 2018

Country	Organization Name	Organizational Model	Scale of Command
Albania	Defense Intelligence and Security Agency	branch	subordinated
Belgium	Cyber Security Operations Centre	branch	sub-unified
Canada	Directorate of Cybernetics	branch	sub-unified
Croatia	Center for Communications and Information Systems	branch	sub-unified
Czechia	National Cyber Operations Centre	branch	sub-unified
Denmark	Computer Network Operations Unit	joint	subordinated
Estonia	Cyber Command	branch	unified
France	Cyber Defense Command Unit	joint	unified
Germany	Cyber and Information Space Command	service	unified
Greece	Joint Cyber Command	joint	unified
Hungary	Cyber Defense Center	branch	sub-unified
Italy	Joint Command for Cyberspace Operations	joint	sub-unified
Luxembourg	Army Cyber Cell	service	subordinated
Netherlands	Defense Cyber Command	joint	unified
Norway	Cyber Defense Force	branch	unified
Poland	Cyber Operations Centre	branch	sub-unified
Portugal	Cyber Defense Centre	branch	subordinated
Romania	Cyber Defense Command	branch	unified
Slovakia	Cyber Defense Centre	branch	sub-unified
Spain	Joint Cyber Defense Command	joint	unified
Turkey	Turkish Armed Forces Cyber Defense Command	branch	sub-unified
United Kingdom	Joint Forces Cyber and Electromagnetic Group	joint	sub-unified
United States	U.S. Cyber Command	joint	unified

TABLE IV: CYBER FORCE STRUCTURE FOR NON-NATO STATES, 2018

Country	Organization Name	Organizational Model	Scale of Command
Argentina	Joint Cyber Defense Command	joint	unified
Australia	Defense SIGINT and Cyber Command	joint	sub-unified
Austria	Command Support and Cyber Defense Command	branch	unified
Bangladesh	Directorate General of Forces Intelligence	branch	subordinated
Belarus	Army Cyber Units	service	subordinated
Brazil	Cyber Defense Command	service	sub-unified
Chile	Joint Cyber Defense Command	joint	sub-unified
China	People's Liberation Army Strategic Support Force	service	unified
Colombia	Joint Cybersecurity and Cyber Defense Command	joint	sub-unified
Ecuador	Cyber Defense Command	joint	unified
Finland	Cyber Defense Division	branch	sub-unified
India	Defense Information Warfare Agency	branch	subordinated
Indonesia	Cyber Operations Command	branch	sub-unified
Iran	Cyber Defense Command	joint	sub-unified
Ireland	Communications and Information Services Corps	branch	subordinated
Israel	Unit 8200	branch	subordinated
Japan	Cyber Defense Unit	branch	sub-unified
Kazakhstan	Cyber Branch	branch	unified
Malaysia	Cyber Defense Operation Center	branch	subordinated
Mexico	Naval Cybersecurity Center	service	subordinated
Myanmar	Military Security Affairs	branch	subordinated
Nigeria	Cyber Warfare Command	service	sub-unified
North Korea	Unit 121	branch	subordinated
Paraguay	General Directorate of Information Technology and Communication	branch	sub-unified
Peru	Cyber Defense Command	service	sub-unified
Philippines	AFP Signal Corps	service	subordinated
Russia	Main Directorate of the General Staff (GRU)	branch	subordinated
Serbia	Command Information Systems and IT Support Centre	branch	subordinated
Singapore	Cyber Defense Group	branch	subordinated
South Africa	Defense Intelligence Division	branch	subordinated
South Korea	Defense Cyber Command	joint	unified
Sri Lanka	Army Signals Corps 12th Regiment	service	subordinated
Sweden	Military Intelligence and Security Service	branch	subordinated
Switzerland	Electronic Operations Centre	branch	subordinated
Thailand	Army Cyber Center	service	subordinated
Ukraine	Main Directorate of Communication and Information Systems	branch	subordinated
Venezuela	Joint Directorate of Cyber Defense	joint	sub-unified
Vietnam	Cyberspace Operations Command	joint	unified