Beyond Threats: How Allies and Bureaucratic Politics Shape Military Cyber Integration

Nadiya Kostyuk*

August 5, 2024

Abstract

The politics of how nations design their militaries when integrating new technologies is a critical question in international relations as it has implications on military effectiveness, civil-military relations, war conduct, power projection, and peace and stability. Cyber is the latest example of a technology that countries have been integrating within their militaries to varying degrees. Yet, there is limited theoretical and empirical work on the factors that explain how nations design their militaries to absorb cyber technologies. Using panel data on state military organizations between 2000 and 2018, this article shows that allies and bureaucratic politics affect the military design choice whereas threats are insufficient in explaining this choice. These results are robust to a number of alternative specifications and generally succeed in out-of-sample prospective predictions. The findings have important implications for the study of national security policy, alliances, and innovation.

*Carnegie Mellon Institute for Strategy and Technology, Carnegie Mellon University; nkostyuk@andrew.cmu.edu

The politics of how nations design their militaries to integrate new technologies is a crucial issue in international relations, impacting military effectiveness, civil-military relations, the conduct of war, power projection, and overall peace and stability (Gannon, 2021; White, 2019). Cyber technology, as a recent example, has been integrated into military structures to varying extents across different countries (Blessing, 2020; Wiener, 2016). Research indicates that a state's decision to incorporate cyber capabilities influences modern warfare, affecting critical factors such as deterrence (Borghard and Lonergan, 2017; Lindsay and Gartzke, 2015), escalation (Borghard and Lonergan, 2019; Kreps and Schneider, 2019), national strategies (Rovner, 2023), and dynamics within alliances (Guenther and Musgrave, 2022; Kostyuk, 2020, 2024). Despite the significant implications of these processes on various global political variables, there remains a notable lack of theoretical and empirical research on how nations design their militaries to effectively integrate cyber technologies.

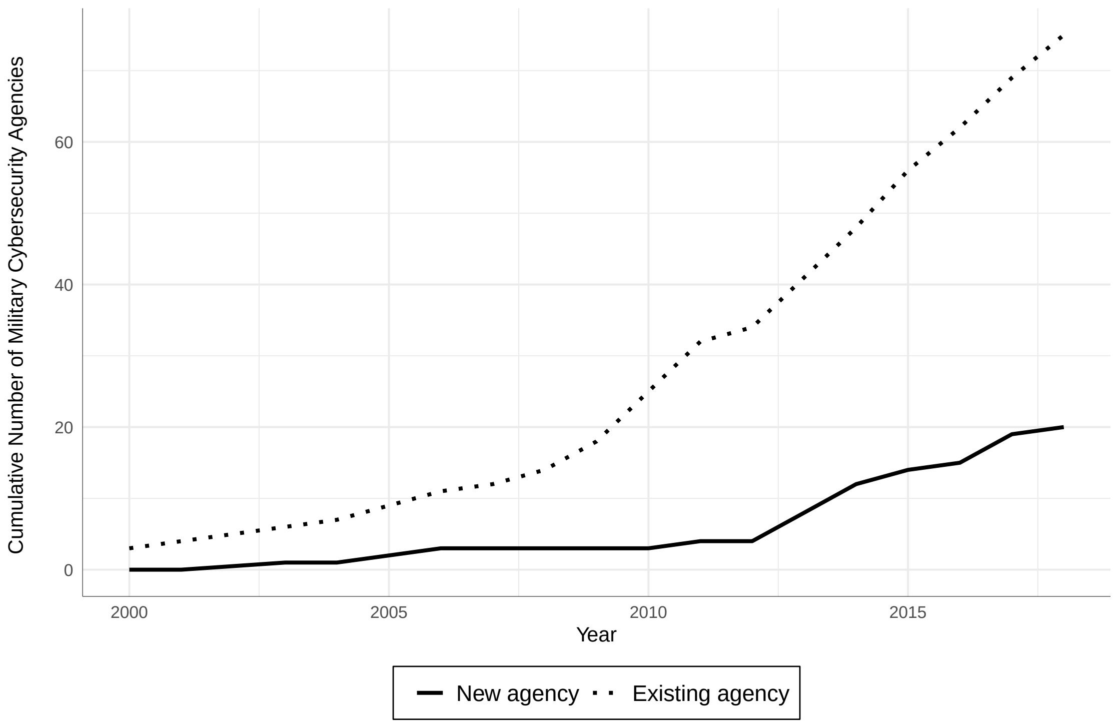
The international relations (IR) literature offers extensive insights into why militaries adopt various technologies (e.g., Most, Starr and Siverson (1989); Jo and Gartzke (2007); Horowitz (2010); Fuhrmann and Horowitz (2017); Kahn and Horowitz (2021); Gannon (2021)). Building on these works, recent scholarship explains why countries acquire cyber capabilities (Gomez, 2016; Valeriano, Jensen and Maness, 2018; Kostyuk, 2024). A few recent works that focus on military cyber organizations explore either why states struggle to create effective cyber organizations (Smeets, 2022) or focus on countries' different force postures (Blessing, 2020; Cunningham, 2022). Building on this scholarship and extending it further, this article investigates the variation in how countries institutionalize their military cyber capabilities and the organizational choices they make during the development of these new technologies.

As with any technology, the military can incorporate cyber in one of the two ways: (1)

add these new capabilities to an existing agency or (2) create a new agency responsible for the development of these capabilities. In the former case, the military acquires cyber capabilities to provide combat support for its ground operations, for instance, making cyber capabilities an integral part of its army. In the latter case, the military creates a cyber force with its own separate mission of withstanding and responding to cyber attacks. While the military can pursue both options sequentially, this research investigates which option it chooses first. Delegating responsibility to an existing agency allows a country to quickly begin working on new capacity development, but it can be difficult to optimize the development of operational capacity. Creating a new agency, on the other hand, takes more time and resources, but it more effectively increases the new capacity. For instance, at the 2010 hearing of the U.S. Committee on Armed Services, the committee chairman described the creation of the U.S. Cyber Command as "a critical milestone for our Nation's defense" and stressed its significance for the "military's ability to conduct its operations in cyberspace" given that the command incorporated all cyber efforts within the department "under one vision and one mission" (U.S. House of Representatives, 2009).

Figure 1 illustrates the initial choices countries made when beginning to develop cyber capabilities within their military organizations from 2000 to 2018. It shows that seventy-five countries opted to integrate these capabilities into existing agencies, while twenty chose to establish new agencies. This suggests a preference for incorporating cyber capabilities into existing military structures. This observation raises key questions: *What explains this preference?* Specifically, *why do most countries expand their cyber capabilities within existing military agencies, even though creating new agencies might more effectively enhance operational cyber capacity?* Conversely, *why do some countries choose to create new units, despite the higher costs and longer path to achieving operational capacity?* Understanding the rationale behind these choices is essential, as each option impacts military operations, readiness, and effectiveness in different ways.

Figure 1: INITIAL INTEGRATION OF CYBER TECHNOLOGIES WITHIN MILITARIES OVER TIME: EXISTING VERSUS NEW AGENCIES



Note: The figure displays the choice countries made over time when they started integrating cyber technologies within their militaries. *New agency*—nations developed brand new agencies with a sole responsibility of cybersecurity. *Existing agency*—nations assigned their existing agencies to deal with cybersecurity. The lines display a cumulative number of countries that made this choice in a given year. As of 2018, seventy-five countries used existing agencies and twenty created new agencies *Source:* Author's calculations based on Kostyuk (2022)'s State Cybersecurity Organizations (SCO) data (v1.0).

Studying how and why states begin integrating cyber capabilities into their militaries is important for four key reasons. First, the unique characteristics of cyber weapons—such as their transitory nature, which affects their time-dependent effectiveness (Buchanan and Cunningham, 2020), and their high asset specificity, which limits their redeployment (Williamson, 1991)—may influence how states conduct operations, project power, and build security. Understanding these dynamics is crucial for scholars and policy-makers. Second, as many countries have only recently begun developing their cyber arsenals, this research provides valuable insights into how they incorporate cyber capabilities into military strategies and offers a unique opportunity to identify the key drivers and predict the future evolution of this technology. Third, applying theories of weapon proliferation to new cases can enhance our understanding of the proliferation process and its global political implications. Lastly, media reports often make bold claims about cyber capacity based on speculation rather than rigorous empirical analysis. This research addresses these speculations and offers important lessons for policymakers.

To identify a few potential mechanisms that can systematically explain how states start integrating cyber technologies within their militaries, I build on works that have applied the interest-capacity framework to explain the diffusion of new technologies (e.g., (Jo and Gartzke, 2007; Fuhrmann and Horowitz, 2017; Kahn and Horowitz, 2021)). I supplement existing explanations identified in the literature with evidence from sixty-four semi-structured interviews conducted in 2018 with cybersecurity experts who have current or past government affiliations—many of whom have connections to the military—from twenty-five countries.[1] I hypothesize that both supply- and demand-side factors systematically influence this process and test theories related to the threat environment, the influence of allies, and interservice rivalries.

I test my hypotheses using Kostyuk (2022)'s panel data on state cybersecurity organizations for the 2000-2018 period. I find that allies and interservice rivalries most consistently explain a country's choice of how to incorporate cyber technologies. The results suggest two competing influences of allies. On the one hand, countries imitate their allies' cyber capacity by starting to develop cyber capabilities within existing military agencies. On the other hand, countries complement their allies' cyber capacity by starting to develop cyber capabilities within a new military cyber agency. When there is greater equality among military services, countries are likely to create a new agency for integrat-

[1] The IRB approval is #HUM00127749 (February 14, 2018).

ing cyber technologies. While my results present only correlations—not causation—they withstand a number of robustness checks. Importantly, my model succeeds in predicting which countries will next integrate cyber technologies within their militaries (i.e., out-of-sample prospective predictions).

These findings make five important contributions to the political science literature. First, they advance the scholarship on cyber capacity proliferation by explaining the variation in operational cyber capacity resulting from different approaches to integrating cyber technologies within militaries. Second, they enrich the literature on the spread of military technologies and innovation by demonstrating that threats alone do not fully explain how nations integrate cyber technologies. Instead, domestic and international factors, such as interservice rivalry and the influence of allies, offer a more consistent explanation. Third, they contribute to understanding diversification and specialization within alliances (e.g., by exploring how these phenomena manifest in the cyber domain. Fourth, they enhance the civil-military relations, and military effectiveness literatures by highlighting the crucial role of internal power dynamics in developing cyber capabilities and their impact on operational effectiveness and combined arms approaches. Last, this study adds to the political science literature on diffusion by examining the timing of competing choices countries make when integrating new technologies, offering deeper insights into the factors shaping defense policies and their implications for global politics.

Literature Review

The IR literature provides extensive insights into why militaries adopt various technologies (e.g., Most, Starr and Siverson (1989); Jo and Gartzke (2007); Horowitz (2010); Fuhrmann and Horowitz (2017); Kahn and Horowitz (2021); Gannon (2021)). These studies typically focus on the adoption of specific systems or artifacts, such as tanks or drones. Cyber, however, presents a distinct case due to its broader and more complex nature. It is so intricate that it has been conceptualized with its own set of domain assumptions (Lupovici, 2016; Branch, 2021), even as it overlaps with intelligence and other domains (Lindsay, 2021).

Building on these existing works, there is a growing body of theoretical and empirical research that explores why nations develop their cyber capabilities. This next group of scholars zeroes in on a more focused interpretation of cyber—the concept of "state military cyber capacity" (Gomez, 2016; Valeriano, Jensen and Maness, 2018; Kostyuk, 2021, 2024). Kostyuk (2024, 46) defines *state military cyber capacity* as "the ability of a nation-state's military to effectively conduct operations in cyberspace, including the defense of its own networks and systems from cyber threats and the execution of offensive cyber operations for various purposes, such as intelligence gathering and disruption of adversarial networks." For this article, I adopt this definition and analyze how countries choose to organize their military in the development of this capacity.

Most research on the diffusion of military cyber capabilities has focused on their *use*—specifically, executed cyber operations (e.g., Valeriano, Jensen and Maness 2018). Recently, however, attention has shifted to the *institutionalization* of cyber capacity, focusing on the organizations states develop to build this capacity (Kostyuk, 2024). This latter focus has notable advantages. Unlike non-reproducible cyber-operations that exploit isolated, time-limited vulnerabilities, institutional developments offer a publicly visible increase in organizational capacity, demonstrating a state's consistent ability to produce cyber weapons (Kostyuk, 2021). Building on this scholarship, this article extends the discussion by examining the variation in *how* countries *institutionalize* their military cyber capabilities. Put simply, rather than focusing solely on instances when countries deploy their "cyber weapons," this article investigates how militaries choose to develop these weapons. This approach provides a deeper understanding of how militaries plan and execute their behavior in cyberspace.

The topic of the emergence and selection of military cyber organizations is relatively new in the IR literature. However, three key works are particularly relevant. First, Smeets (2022)' people-exploits-tools-infrastructure-organization (PETIO) framework offers several resource-based logics of why states struggle to establish effective military cyber organizations. This framework provides insights into factors influencing the decision to place cyber capabilities within existing or new organizations. However, the PETIO theory remains relatively agnostic about how states specifically address these resource challenges through organizational choices. Second, Blessing (2020) also remains neutral on the question of whether to establish new or integrate cyber capabilities into existing organizations. While this study, like the current article, examines adoption dynamics, it focuses more on the broader issues of force structure creation rather than the establishment of cyber-specific organizations. Lastly, Cunningham (2022)'s theory of strategic substitution primarily investigates China's adoption of various force postures, rather than examining the global patterns of creating cyber-specific organizations.

Until now, the literature has largely overlooked how militaries begin developing their cyber capabilities. This study addresses this gap. Understanding how states initiate the development of cyber capabilities within their militaries is crucial because it has significant implications for peace and security. It impacts civil-military relations, influences operational conduct, affects power projection, and alters various other dynamics of modern warfare.

The initial choice to develop military cyber-capacity: Existing versus new agencies

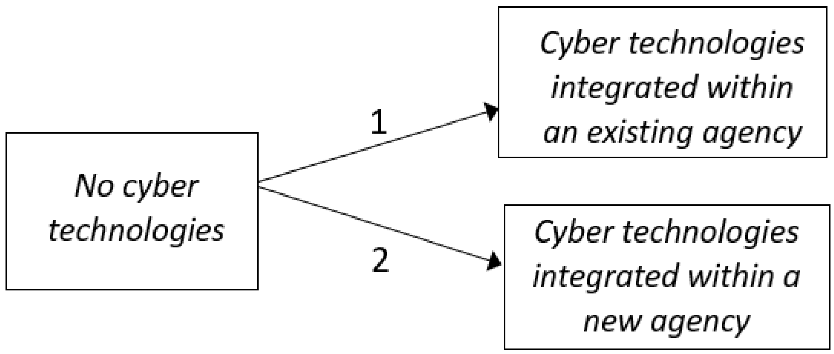
How do militaries incorporate new technologies? Let us consider the example of airplanes. A military can integrate airplanes into its existing branches to support ground operations, making them a crucial part of the current army structure. Alternatively, the military can establish a new branch, such as an air force, dedicated specifically to aerial missions like bombing and air combat. This example illustrates that when a new technological capability arises, the military can either assign the responsibility for this capability to an existing agency (e.g., integrating space operations within the Air Force) or create a new, specialized agency focused solely on the development of this capability (e.g., forming a Space Force as a separate service branch).

Countries have these two main choices when they consider developing their military cyber-capabilities. Figure 2 displays two ways in which how a state that lacks cybercapacity can start integrating cyber technologies. First, a state can do it within an existing agency[2] by adding new cyber responsibilities to the agency's mission. For instance, in addition to ensuring the safety of Albanian maritime space, the Albanian Ministry of Defense's Inter-institutional Maritime Operational Center (IMOC) became responsible for the development of cybercapacity. Second, a state can create a new agency whose sole responsible is cybersecurity. For instance, the Japanese Self Defense Forces' Cyber Defense Unit's duty is "monitoring information and communications networks and responding to cyber attacks on a round-the-clock basis."[3]

[2]Since different armed forces, and even different branches of service of the armed forces, may use the same name to denote different types of organizations, I use "agency" to avoid any confusion. By "agency" I mean an "active-duty military organization with the capability and authority to direct and control strategic cyberspace operations to influence strategic diplomatic and/or military interactions" (Blessing, 2021, 235).

[3]For more information, please visit the website of the Japanese Ministry of Defense:

Figure 2: INTEGRATING CYBER TECHNOLOGIES: COMPETING RISKS SCHEME



Importantly, both choices identify the initial step of cybercapacity development that generally takes place within any military branch and does not explain the full evolution of the capacity development that can take the form of a combatant command, for instance.[4] Despite this, studying how a state chooses to start integrating cyber technologies within its military is important because this choice explains how a country decides to organize its cybercapabilities and how this newly-developed bureaucratic capacity will translate into operational capacity, communicating a country's level of commitment to develop its ability to inflict pain and defend itself and allies via cyberspace.

Each choice has its pros and cons. Developing cyber capabilities within an existing agency allows a country to start working on this capacity more quickly. However, optimizing the agency's operations in this new area can be challenging due to the need to adapt its standard operating procedures. Assigning cybersecurity responsibilities to an existing military agency requires significant mutual adaptation, affecting both innovation and organizational change. For example, as IMOC takes on new cyber responsibilities, it must adjust its approach to safeguarding maritime space, while its organizational culture influences the development of its cyber defenses. This dual adjustment can impact the

https://www.mod.go.jp/e/publ/answers/cyber/index.html

[4]See Blessing (2020) for the explanation of the cyber military force structure.

agency's overall performance against each challenge. Furthermore, adding new cyber responsibilities to an existing military agency can lead to mission creep, introducing unwarranted complexity and potentially blurring the agency's core mission. This, in turn, can slow down the development of operational cyber capacity and reduce the agency's effectiveness on the battlefield (Kostyuk and Gartzke, 2022*b*).

On the other hand, if military operations span multiple domains, integrating cyber technologies into an existing agency may facilitate better force synchronization compared to creating a separate agency, which often encounters bureaucratic barriers in coordinating with others. Additionally, adding cybersecurity responsibilities to an existing agency can streamline information sharing and collaboration, whereas establishing a separate agency may complicate these processes.

Creating a new military cyber agency can be highly beneficial, particularly given the unique characteristics of cyber technologies. Cyber technologies, with their high asset specificity, require significant technical expertise that must be continuously updated and maintained. Unlike physical assets such as tanks, which have low specificity and can be used effectively regardless of who operates them, cyber operations are highly specialized. They often need to be tailored to specific networks and vulnerabilities (Buchanan and Cunningham, 2020). The creators of cyber tools generally possess a deeper understanding of their products compared to those who merely acquire or use them. Therefore, having a dedicated cyber agency ensures that the organization can develop and manage these technologies with the required expertise, leading to better overall effectiveness of independent cyber capabilities in the long run.

Creating a new military cyber agency is not without a number of challenges. First, it generally requires more time and resources than integrating cybersecurity responsibilities into an existing agency. Establishing a new agency involves setting up new infrastructure, recruiting and training personnel, and developing new operational protocols, which can be both costly and time-consuming. Additionally, new agencies often face initial inefficiencies as they build their internal processes and integrate new systems. Second, a newly established agency may encounter significant bureaucratic hurdles, including inter-agency coordination challenges and resistance from existing agencies that might perceive it as a threat to their authority or resources. This can lead to delays and complications in implementing effective cyber strategies. Third, creating a new agency can lead to fragmentation of efforts and lack of synergy with existing military operations, potentially undermining the effectiveness of cyber capabilities due to difficulties in coordinating across different branches and units. Finally, the establishment of a new agency might result in a lack of immediate integration with established military practices and cultures, which can affect its operational efficiency and ability to quickly adapt to evolving cyber threats.

Given that each choice has its pros and cons, it is important to understand the factors that influence this decision. The next section will explore the mechanisms likely to affect how and why a state chooses between integrating cyber capabilities within existing agencies or creating a new agency dedicated to this task.

Explaining Initial Integration of Cyber Technologies

Scholars have applied the interest-capacity framework to explain various international relations phenomena, including democratization, war, central bank independence, and international economic organizations (Bodea and Hicks, 2015; Gleditsch and Ward, 2006; Simmons, Dobbin and Garrett, 2008; Siverson and Starr, 1990). They have also used this framework to explain adoption of a new technology, focusing on the *interests* or *willingness* of relevant actors in acquiring it (i.e., demand-side factors) and the *capacity* or *op-*

portunity of these actors to develop or obtain this technology (supply-side factors) (Most, Starr and Siverson, 1989; Jo and Gartzke, 2007; Fuhrmann and Horowitz, 2017). Using this framework, scholars consider a number of demand- and supply-side factors that affect a country's decision to develop military cybercapacity, including threats and rivalry, elite influence, Internet reliance, regime type, prestige, influence of allies, among others (Gomez, 2016; Brantly, 2016; Calderaro and Craig, 2020). These works generally focus on a binary choice—capacity development or its lack. Many of them are country-specific (Tabansky, 2020) or region-specific (Brantly, 2016). Building on this scholarship and extending it a step further I explain how the initial choice to integrate cyber technologies takes place.

To identify a few potential mechanisms that can systematically affect this process, I supplement existing explanations identified in the literature with the evidence from sixty-four semi-structured interviews conducted in 2018 with cybersecurity experts with a current or past government affiliation—many of them have connection to the military—from twenty-five countries.[5] The main purpose of these interviews was theory building and not theory testing. Below, I discuss a few potential mechanisms—threat environment, influence of alliances, and interservice rivalry.

Threat environment. Countries often develop new capabilities in response to international threats (see, e.g., Jervis 1978; Waltz 1979; Posen 1993; Resende-Santos 2007). The security dilemma, where "one state's gain in security often inadvertently threatens others" (Jervis, 1978, 170), creates incentives for nations to innovate. A state concerned about the size and effectiveness of its capabilities relative to its rival might imitate the same capabilities as its rival in order to effectively counter its enemy's strategy (Resende-Santos, 2007; Evangelista, 1984). Cybercapabilities are no exception. Past research shows states' con-

[5] Online Appendix Section add provide a detailed explanation of the interviews I conducted for this project.

cerns about cyber-threats as a cybercapacity driver (Gomez, 2016; Calderaro and Craig, 2020). The interviews that I conducted with cybersecurity experts further corroborate this reasoning and provide anecdotal evidence that ongoing disputes or tense relations with China and Russia, for example, trigger countries to start developing their military cybercapacity (e.g., Interview, 2018: #3, #11, #35).

As a result, a state concerned with an enemy's growing cybercapabilities is likely to pay attention to the enemy's cyber institutions and might wish to structure its forces similarly to this enemy to be better prepared to fight them in cyberspace. For instance, a Finnish security analyst explains the role Russia plays in how Finland approaches the development of its military cybercapacity: "Our thinking is to some degree impacted by the only potential mortal threat that we might have to face at some point in time, Russia...Their view on cyber differs from most of the Western nations...As we have to be prepared to operate effectively against our adversaries, we also have to be able to think like they are thinking and be able to utilize also their concepts and ideas. Thus...Russian way of seeing cyber has had some impact on our thinking, particularly in the military domain" (Interview, 2018: #16). Since adversaries' cyber institutions are likely to shape a country's military cyber institutions (e.g., Interview, 2018: #3, #11, #35), I propose the following hypotheses:

> **H1A:** *Countries are more likely to start developing their cyber capabilities by incorporating them within existing military agencies when their adversaries have similarly incorporated new cyber capabilities within their existing military agencies.*
>
> **H1B:** *Countries are more likely to start developing their cyber capabilities by creating a new military cyber agency when their adversaries have similarly created new cyber agencies.*

Influence of Allies. Besides building arms, states also form alliances to balance against external threats (Waltz, 1979). Research shows that allies have an incentive to share and transfer their capabilities to weaker alliance members in order to increase an alliance's overall security (Yarhi-Milo, Lanoszka and Cooper, 2016). Given this incentive, allies are likely to play a role in whether and how states decide to integrate cyber technologies within their militaries. Kostyuk (2024) shows that allies are particularly important in the process of cybercapacity development because they serve as a supplier of information and training. Specifically, to increase an alliance's overall security, a country's ally that already possesses cybercapabilities is eager to help the country develop its own cybercapacity. Given cyber tools' transitory nature, which makes their effective use strongly time dependent (Buchanan and Cunningham, 2020), an ally is not willing to share these exact tools with a country. Instead, an ally shares its knowledge and expertise in the form of training and joint military exercises,[6] and help with institution-building (Smeets, 2022).

An ally's willingness to share information about its institutions creates an additional incentive for a nation to imitate these institutions when developing cybercapacity of its own so states can more effectively tackle common threats. For instance, when developing its cybersecurity apparatus, Denmark paid close attention to what Germany and the Unites States were doing and modeled its cybersecurity organizations after these countries' organizations (Interview 2018: #50). Norway is known to "copy" the U.K.'s cyber institutions (Interview 2018: #11). South Korea designed its cyber command after the U.S. The same Finnish security analyst who explained the role rivalries play in Finland's process of developing cybercapacity also elaborated on an important role of the country's allies in this process: "As we work together with the US and NATO..., it is clear that it must have had its impact on our way of viewing cyber and information domain. In or-

[6] I would like to thank an anonymous reviewer for pointing out that during these exercises countries and their allies are working on integrating their cyber capabilities to be used in joint/combined military operations.

der to be able to operate together with like-minded countries, we have to share concepts, organizational structures, ways to conceive operations, etc." (Interview, 2018: #16). Since allies are likely to shape a country's military cyber institutions (e.g., Interview 2018: #12, #2, #35), I propose the following hypotheses:

> **H2A:** *Countries are more likely to start developing their cybercapabilities by incorporating them within existing military agencies when their allies have similarly incorporated new cybercapabilities within their existing military agencies.*

> **H2B:** *Countries are more likely to start developing their cybercapabilities by creating a new military cyber agency when their allies have similarly created new cyber agencies.*

Bureaucratic Politics & Interservice Rivalry. Research shows that bureaucratic politics can also affect how militaries incorporate new technologies (Huntington, 1961; Allison and Morris, 1975; Brown, 2019; Neufeld, 2005; Grauer, 2015). In discussing bureaucratic politics, Allison and Halperin (1972) highlights a bargaining process that occurs among different players within a bureaucracy.[7] I focus on bureaucratic competition, specifically interservice rivalry, as an example of this bargaining process.

On the one hand, services might be eager to incorporate new technologies because they open new warfighting possibilities often creating an expectation of a cheap victory (Rovner, 2023). But this expectation is not always fulfilled because new technologies

[7] According to Allison and Halperin (1972, 43), constraints such as organizational processes, shared values, and organizational culture can significantly impact the bargaining process. However, exploring how these constraints shape the bargaining process falls outside the scope of this paper, as the current research design, which focuses on explaining global trends over time, does not allow for testing these additional mechanisms. Focusing on the case of the United States, White (2019) illustrates how subcultures within different military services influence the development of U.S. military cyber doctrine. Additionally, Kostyuk, Perkoski and Poznansky (2022) highlight the importance of organizational culture in shaping U.S. cyber strategy. Future research should examine both organizational culture and organizational processes—defined as standard operating procedures (SOPs) and organizational routines that shape governmental decisions—as potential explanations for the creation of cyber-relevant military organizations.

do not always translate into better military effectiveness. The development of an anti-ballistic missile (ABM) system to defend the United States against intercontinental ballistic missile (ICMB) strikes expected from China is such an example. In 1969, President Nixon modified the Sentinel ABM program proposed by President Johnson to the Safeguard ABM program. This change resulted in a shift from a light ABM system meant to defend against ICBM strikes to a hybrid area-defense and terminal-defense meant to defend cities. Pressure from the army was the reason for the development of this program which was worse at defending ICMB silos. Being in charge of defending the U.S. from enemy air attack, the army wanted a role in nuclear issues. They felt that the ABM program was their last chance to have this role. If developed, the Sentinel ABM was likely to end up under the Air Force since this program meant to protect ICBMs rather than cities (Allison and Morris, 1975).[8]

One the other hand, bureaucracies might be reluctant to incorporate new technologies because innovations add new missions that consume time and resources devoted to a service's existing responsibilities and main priorities. Even though the U.S. Air Force (USAF) showed little enthusiasm for the A-10C Thunderbolt II— the first Air Force aircraft specially designed for close air support (CAS) of ground forces—its acquisition enabled the USAF to pursue the F-15, an all-weather tactical fighter aircraft which allowed the USAF "expand its active fighter force structure" (Dahl, 2003, 8). Despite that the A-10 remained unpopular among the USAF because they felt like they were the army's bodyguard while conducting CAS; instead, they would have liked to spend more time pursuing their own missions (Dahl, 2003).

Preliminary anecdotal evidence from a survey of existing scholarship and my interviews suggests that bureaucratic politics and interservice rivalry seem to play a role in

[8] In addition to army preferences, domestic politics also played a role in this situation (Rovner, 2023).

how military decide to integrate cyber technologies (e.g., Tabansky 2020, Interview, 2018: #9, #17, #27, #36, #39). If so, how do the competing priorities outlined above play out when it comes to cyber technologies?

Let us examine the warfighting mechanism through which interservice rivalry can shape military cyber organizations. As with any new technology, cyber offers new warfighting opportunities. But unlike other technologies, cyber-operations can uniquely serve as both a complementary tool for tactical military operations and a substitute for military force.[9] The complementarity advocates explain that well-executed cyber-operations provide an efficient and quick way of corrupting enemy communications and disrupting their battlefield effectiveness (Liff, 2012). The substitution advocates argue that states can use cyber-operations to degrade or destroy enemy capabilities in peacetime (Valeriano, Jensen and Maness, 2018). Importantly, leaders can deny responsibility for these operations; as a result, they face a lower chance of retaliation from the target, as well as limiting blowback at home, compared with traditional tools. Given this peculiarity, cyber technologies are alluring because they provide a more efficient and cheap way of achieving an agency's objective using cyber-operations either exclusively or in tandem with the agency's conventional tools.

Resource constraints are another mechanism through which interservice rivalry can shape military cyber organizations. On the one hand, developing cyber capabilities within an existing agency might consume time and resources that are already devoted to the service's core responsibilities and priorities. On the other hand, integrating cyber capabilities into a service's portfolio could open up opportunities for additional resources. This latter logic seems to be common among my interviewees. For instance, as a Danish security analyst explains: "Cyber is sexy. Organisations fight to get 'cyber' under their umbrella as

[9] The efficiency of cyber-operations as complements and substitutes remains out of the scope of this paper. For a review of these debates, see Kostyuk and Gartzke 2022*a*.

‘cyber’ means more funding” (Interview, 2018: #23). However, this additional funding for cyber does not necessarily translate into new missions that are distinct from an agency’s current objectives. Instead, it provides new means to achieve the agency’s existing goals.

Using this explanation, I argue that agencies generally seem to be eager to develop cybercapabilities. Research shows that if a particular agency has more influence, they are likely to obtain a monopoly over these capabilities. For instance, due to its historical focus on intelligence collection using computer and Internet methods, the U.S. National Security Agency kept a monopoly over cybercapabilities during the 2000s (Kostyuk, Perkoski and Poznansky, 2022). Among all U.S. services, the Air Force played “an instrumental role in the development of computing technologies, and consequently embraced the operational potential of cyberspace well over a decade before the other services” (White, 2019, 170). But when agencies have equal influence and each desires control over cyber capabilities, I argue that politicians might opt to create a new agency, effectively distributing the control to no one in particular. *Hypothesis 3* summarizes this logic.

> **H3**: *Countries who do not have one dominant service within their military are more likely to start incorporating cyber technologies by creating a new cyber agency.*

Data & Empirical Strategy

This section briefly introduces my data and empirical strategy. Online Appendix Section 2 include more details.

Dependent Variable: Initial choice to start developing cyber-capabilities within militaries

Since I am interested in a competing choice a country makes when it starts integrating cyber technologies within its military (Figure 2), my dependent variable receives a "1" when a country starts developing cyber-capabilities within an existing military agency (`Existing`), a "2" when it starts developing them within a new military agency (`New`), and a "0" if it does nothing during the 2000-2018 period. To create my dependent variable, I use Kostyuk (2022)'s State Cybersecurity Organizations (SCO) data (v1.0). To identify relevant military agencies from the SCO dataset, I follow Kostyuk (2024)'s approach, which defines "a military agency" as including both active- or reserve-duty military organizations or civilian defense agencies responsible for developing and implementing military cyber organizations." Using this approach, an example of what I code as a "1" would be Luxembourg's Directorate of Defense becoming responsible for developing capacity against cyberattacks (*Defence Guidelines for 2025 and Beyond*, 2017, 12). An example of what I code as a "2" would be building the Operational Center for Cyber Defense within Bulgaria's armed force meant to "respond to cyber and hybrid effects of national and international scale" (*National Cybersecurity Strategy*, 2016, 42-43).[10] Out of 159 nations included in the analysis,[11] seventy-five countries used existing agencies and twenty countries created new agencies.

[10] It is worth noting that civilian defense agencies, like the Luxembourg's Directorate of Defense, are a higher-level proxy measure for cyber in the military.

[11] I exclude countries that do not have militaries (e.g., Costa Rica). Due to the data missingness in some covariates, some countries did not make it to the final sample.

Main Predictors

My theoretical explanation considers three possible drivers of how states choose to integrate cyber technologies: (1) the influence of adversaries who have already started integrated these technologies; (2) the influence of allies who have already started integrated these technologies; and (3) interservice rivalry.

Influence of adversaries. Since states can attack each other using cyber and/or conventional means, I identify adversaries using Diehl, Goertz and Gallegos (2021)'s Peace Data (v3.01)[12] and Valeriano, Jensen and Maness (2018)'s Dyadic Cyber Incident Dataset (DCID) (v1.5). I use Kostyuk (2022)'s SCO data to record where adversaries started integrating cyber technologies. Since I consider the impact of two choices adversaries can make when they start integrating cyber technologies—placing them within *existing* or *new* agencies—I create the following two variables. First, *Adversaries Integrating Cyber Technologies within Existing Agencies* identifies an impact of the fraction of adversaries who started integrating cyber technologies within existing agencies. Second, *Adversaries Integrating Cyber Technologies within New Agencies* identifies an impact of the fraction of adversaries who started integrating cyber technologies within existing agencies.

To capture the fraction of a country's adversaries that have begun developing their cyber capabilities through existing or new military agencies, I avoid the complexity of lagging the dependent variable by one period at a time and adding numerous regressors to my model. Instead, I use the approach outlined by Simmons and Elkins (2004), applying lagged network-weighted effects to represent the weighted average of a country's adversaries' initial cyber capacity development. This method accounts for the impact of

[12] This data covers rivalries who have active war plans, frequent militarized disputes, absent communication, and no diplomatic recognition or diplomatic hostility. As an alternative, I also use Maoz (2005)'s data on Militarized Interstate Disputes (MID) to identify adversaries.

adversaries by assigning weights according to their significance. For instance, if a country faces only one adversary, that adversary's influence is weighted at 100%, indicating a major impact on the country's military decisions. In contrast, if a nation has twenty adversaries, each with a weight of 5%, the influence of any single adversary on the country's military decisions is relatively limited. Additional details on the calculation of this weighted average effect are provided in Online Appendix Section 2.1.

Influence of allies. To measure the influence of allies, I use Leeds et al. (2002)'s Alliance Treaty Obligations and Provisions (ATOP) to identify allies[13] and the SCO data to record where allies started integrating cyber technologies. Similarly, I create the following two variables to account for the impact of allies. First, *Allies Integrating Cyber Technologies within Existing Agencies* identifies an impact of the fraction of allies who started integrating cyber technologies within existing agencies. Second, *Allies Integrating Cyber Technologies within New Agencies* identifies an impact of the fraction of allies who started integrating cyber technologies within existing agencies.

To capture the fraction of a country's allies that have begun developing their cyber capabilities through existing or new military agencies, I similarly use Simmons and Elkins (2004)'s lagged network-weighted effects. This method, also utilized in recent studies on state military cyber capacity (Kostyuk, 2024), accounts for the influence of allies by assigning weights based on their significance. For example, if a country has only one ally, that ally's influence is weighted at 100%, meaning their impact on the country's military decisions is substantial. Conversely, if a nation has twenty allies, each with a weight of 5%, the influence of any single ally is comparatively minor. Further details on the calculation of this weighted average effect can be found in Online Appendix Section 2.1.

[13] I also use Correlates of War (COW) Project's data on formal alliances (v4.1) to identify alliances (Gibler, 2008).

Interservice rivalry. To account for the impact of interservice rivalry, I create *Service Dominance* that ranges between 0 and 1, where 0 stands for "no dominance" and 1 stands for "complete dominance." To create this variable, I use Gannon and Kostyuk (2024)'s panel data on a number of troops within each service branch collected from the International Institute of Strategic Studies' Military Balance database. Given that alternative indicators (e.g., budget allocation across services) are not available, military personnel is a commonly used estimator of military capacity (Walter, 2006) and, thus, is a good proxy of dominance among services. I assume that the more balanced troops distribution is, the higher the likelihood of interservice rivalry and, as a result, the lower the value of *Service Dominance* is. To create *Service Dominance*, I find the proportion of troops belonging to each country's largest service within each year. I converge this number to the percentile across countries. The highest value of this variable receives a "1" for the country whose largest service has the highest percentage of troops across all countries within a year and the smallest value receives a "0" whose largest service has the smallest percentage of troops across all countries within a year. The values in-between are distributed between 0 and 1.

Controls

Besides my main predictors, I also account for a country's GDP per capita. Since creating a new agency is more resource-intensive as earlier explained, I hypothesize that wealthier nations might pursue a more expensive option. I account for the country's wealth measured by a country's GDP per capita (logged), taken from the World Bank (GDP per capita).

Method: Competing risks event history model

I use a competing risks event history model.[14] Specifically, I employ a Cox Proportional-Hazards (CPH) model that tests for conditions that create a greater likelihood that a country started integrating cyber technologies. I use a competing risks model because the country chooses to incorporate them within either: (1) an existing agency or (2) a new agency (as shown in Figure 2). My unit of analysis is the country-year. Following existing research (Blessing, 2020), the analysis begins in 2000 shortly after the Internet became a global commercial network. The analysis ends in 2018. If a country has not started integrating cyber technologies within its military by December 31, 2018, it is right-censored in my dataset. Since many of the covariates change over time, I use interval censoring to capture time-varying covariates (Therneau and Grambsch, 2000). Online Appendix Section 2.2 discusses this model in detail and provides additional tests that confirm that the model assumptions are met.

Findings

My central finding is that allies and interservice rivalry most consistently explain a country's choice of whether and how to incorporate cyber technologies. The results summarized in Table 1 suggest two competing influence of allies. On the one hand, countries imitate their allies by incorporating cyber technologies within existing military agency. On the other hand, countries complement their allies by incorporating cyber technologies within a newly-created military cyber agency. When there is a greater equality within military services, countries are also likely to create a new agency for integrating cyber technologies. I discuss these results in details below.

[14]Event history models have been widely used in political science to explain diffusion processes (Berry and Berry, 1990; Elkins, Guzman and Simmons, 2006; Simmons and Elkins, 2004; Simmons, Lloyd and Stewart, 2018).

Table 1 presents the obtained results.[15] Each model in this table considers the competing choice that a country makes when it starts integrating cyber technologies: (1) to place them within an existing agency (*Event: Existing*; column one in each model) or (2) to create a new cyber agency (*Event: New*; column two in each model). The first three models in Table 1 individually consider three primary explanations that I outlined in the theory section—the influence of adversaries (Model 1), the influence of allies (Model 2), and interservice rivalry (Model 3). Model 4 considers the cumulative impact of all these factors with additional controls. Since Model 4 has the highest model fit (concordance = 0.749), I focus on this model when discussing the obtained results.

In Model 4, the impact of adversaries' choices are not statistically significant. These results suggest that a country is unlikely to imitate adversaries when it starts integrating cyber technologies within military, refuting *H1A* and *H1B*. *Allies Integrating Cyber Technologies within Existing Agencies* is positively and statistically significantly correlated with

[15] I use hazard ratios to present my results. Hazard ratios (HR) larger than one identify positive correlation and those smaller than one identify negative correlation.

Table 1: INFLUENCE OF ADVERSARIES, ALLIES, AND INTERSERVICE RIVALRY ON A COUNTRY'S DECISION TO START INTEGRATING CYBER TECHNOLOGIES (HAZARD RATIOS AND CONFIDENCE INTERVALS)

	Model 1		*Model 2*		*Model 3*		*Model 4*	
	E: Existing	E: New	E: Existing	E: New	E: Existing	E: New	E: Existing	E: New
Adversaries Integrating Cyber Technologies within Existing Agencies (lag, sc)	1.203*(1.03;1.41)	1.250^(0.99;1.59)	——	——	——	——	1.085(0.93;1.27)	1.079(0.88;1.32)
Adversaries Integrating Cyber Technologies within New Agencies (lag, sc)	1.023(0.86;1.20)	1.110(0.89;1.39)	——	——	——	——	0.95(0.77;1.17)	0.973(0.76;1.25)
Allies Integrating Cyber Technologies within Existing Agencies (lag, sc)	——	——	1.470***(1.27;1.71)	1.442*(1.09;1.92)	——	——	1.48***(1.25;1.77)	1.445**(1.132;1.84)
Allies Integrating Cyber Technologies within New Agencies (lag, sc)	——	——	1.080(0.90;1.30)	1.362^(0.97;1.92)	——	——	0.94(0.77;1.15)	1.153(0.76;1.74)
Service Dominance	——	——	——	——	0.306**(0.14;0.66)	0.096**(0.02;0.45)	0.790(0.35;1.80)	0.308^(0.08;1.25)
GDP_PerCapita (log)	——	——	——	——	——	——	2.005***(1.57;2.57)	2.270***(1.42;3.63)
Clustering by country	✓		✓		✓		✓	
Concordance	0.567		0.688		0.640		0.749	

Note: Results are from a Cox Proportional-Hazards model, a competing risk model in particular. The reported values are the hazard ratios and confidence intervals. Hazard ratios larger than 1 identify positive correlation and those smaller than 1 identify negative correlation. There are 2,470 observations and 94 events. All results are based on two-tailed tests. *E:* event; `Existing` identifies integration of cyber technologies within an existing military agency; `New` identifies integration of cyber technologies within a new military cyber agency; `log:` logarithmized; `lag:` lagged; `sc:` standardized. ^p<0.1; *p<0.05; **p<0.01; ***p<0.001

both *Existing* (HR: 1.48, CI: (1.25; 1.77)) and *New* (HR: 1.445, CI: (1.132; 1.84)), suggesting that allies are likely to influence a country's decision to integrate cyber technologies within both existing and new agencies. The fact that a country follow its allies' lead and starts integrating cyber technologies within existing military agencies provides preliminary support for *Hypothesis 2A*. But the fact that a country decides to start integrating cyber technologies within a new separate cyber agency when its allies started integrating these technologies within existing agencies refutes *H2B*. This result suggests that allies might be diversifying their cyber toolkit and are potentially working on complementing each other's cybercapacity.

Bureaucratic politics only plays a role in a country's decision to develop a new cybersecurity agency. In particular, a negative statistically significant correlation between *Service Dominance* and *New* suggests the more equality exists between military services, the more likely a country is to create a new cyber military agency. This result provides preliminary support for *H3*. Lastly, a country's GDP per capita is positively and statistically significantly correlated with both dependent variables (*Existing*—HR: 2.005, CI: (1.57; 12.57); *New*—HR: 2.270, CI: (1.42; 3.63)), suggesting the richer a country is, the more likely it is to start integrating cyber technologies.

Robustness Checks. My main findings are also robust to: (1) an alternative measure of alliances (the Correlates of War (COW) Project's data on formal alliances (v4.1) (Gibler, 2008)); (2) alternative network specifications (socio-cultural partners and neighbors); and (3) an alternative functional form of the covariates (the inverse hyperbolic sine function). These results provide further support that allies and bureaucratic politics are likely to affect how nations start incorporating cyber technologies within their militaries.

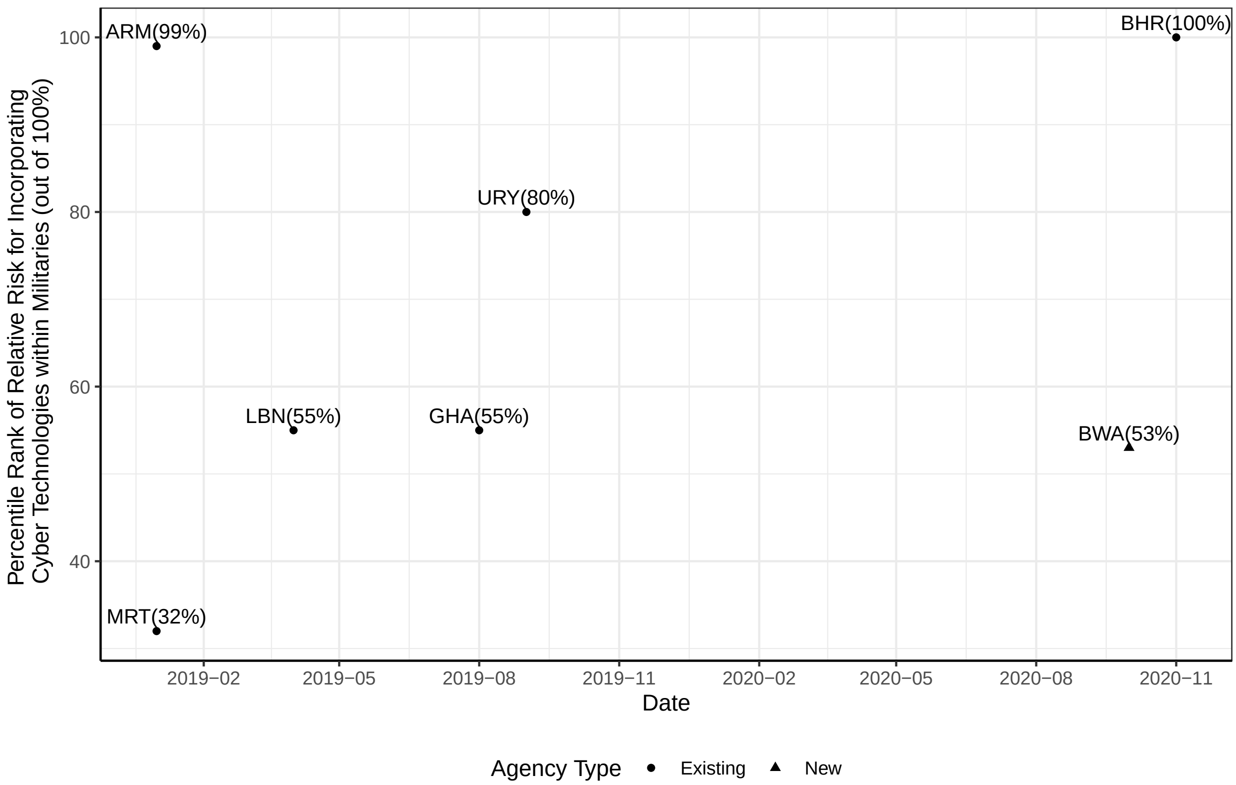
Identifying Future Adopters of Cyber Technologies

To what extent does my model predict future events? I identify the likely candidates for 2019 and 2020, using the estimates from Model 4 (Table 1) trained on data from 2000 to 2018. Figure 3, which depicts the relative rank of countries that started incorporating cyber technologies within their militaries in the years 2019 through 2020, presents the results. The y-axis displays the percentile rank (out of 100%) of relative risk for incorporating cyber technologies as predicted in Model 4 fit using data from the 2000-2018 period. The 2019 and 2020 events are out-of-sample, prospective predictions. Since a CPH model provides predictions of relative (and not absolute) annual risk, I convert relative risk into percentile ranks within each year for ease of interpretation. *Agency Type* identifies how countries started integrating cyber technologies—either within *existing* or *new* military agencies. The obtained results illustrate the potential predictive power of my model. Specifically, of the seven countries that started incorporating cyber technologies in 2019 and 2020 as listed in Figure 3, my model ranks three—Armenia, Uruguay, and Bahrain—at least at 80%. These results provide corroborating evidence to validate my theoretical explanations and demonstrate external efficacy and validity of my model. Not only is my model likely to predict which countries are likely to start incorporating cyber technologies in the future, but it is also likely to predict when and how this process will take place.

Additional Analyses: Explaining the influence of allies

The obtained results reveal an intriguing dynamic concerning the influence of allies on a country's decision to develop its military cyber capabilities. On one hand, states may choose to develop these capabilities within existing military agencies if their allies have

Figure 3: PREDICTIONS: PERCENTILE RANK OF RELATIVE RISK FOR STARTING INCORPORATING CYBER TECHNOLOGIES WITHIN MILITARIES



Note: This plot depicts the relative rank of countries that started incorporating cyber technologies within their militaries. The y-axis displays the percentile rank (out of 100%) of relative risk for incorporating cyber technologies as predicted in Model 4 in (Table 1), fit using data from the 2000-2018 period, making the events occurring in 2019 and 2020 independent look-ahead predictions. This model, a Cox Proportional-Hazards Model, provides predictions of relative (and not absolute) annual risk. I convert the relative risk into percentile ranks within each year for ease of interpretation. *Agency Type* identifies how countries integrate cyber technologies—either within *existing* or *new* military agencies.

already done so, thereby replicating their allies' approach. On the other hand, states might opt to establish a new military agency for cyber capabilities if their allies have implemented these capabilities within existing agencies, thus complementing their allies' approach. What explains this dynamic?

To answer this question, this article builds on the alliance literature that demonstrates that not all alliances are the same. In particular, Leeds (2005) distinguishes between offensive, defense, non-aggression, neutrality, and consultation pacts. Since my analysis starts in 2000, offensive pacts that used to be common in the twentieth century are out of scope. *Defensive* pacts are alliances that assist each other "militarily in the event of attacks on the ally's sovereignty or territorial integrity" (Leeds, 2005, 11). Neutrality pacts, nonaggression pacts, and consultation pacts obligate members to "cooperation short of active military support" (Leeds, 2005, 11). Neutrality and nonaggression pacts promise to "refrain from military conflict with an ally." A neutrality pact commits a member to refrain from assisting an ally's adversary in a conflict. Alliance members who promise neutrality not only commit not to join the conflict against their ally, but also to facilitate their ally's success. Consultation pacts "commit the members to attempt to develop coordinated action" in case of a potential military conflict (Leeds, 2005, 11-12).

Using Model 4 from Table 1 as a base model, I re-ran the results for each type of alliances. Online Appendix Section 5 presents the obtained results. They demonstrate that only defensive alliances (Model 5 in the Online Appendix) exhibit only the replication dynamic, which aligns with the hypothesis proposed by my theory (*H2A* and *H2B*). This is not surprising, as defensive alliances have an incentive to adopt similar structures to facilitate joint exercises.

Neutrality (Model 6 in the Online Appendix) and non-aggression pacts (Model 7 in the Online Appendix) show replication behavior only with respect to existing agencies (i.e., if a country's allies develop cyber capabilities within existing military agencies, the country is more likely to follow suit). Neutrality pacts (Model 6 in the Online Appendix) also exhibit complementarity trends when allies create new agencies (i.e., if a country's allies develop cyber capabilities within new military agencies, the country is more likely to develop capabilities within existing military agencies). Non-aggression pacts (Model 7 in the Online Appendix) display complementarity trends for allies' existing agencies (i.e., if a country's allies develop cyber capabilities within existing military agencies, the country is more likely to develop capabilities within military agencies). Lastly, consultation pacts show replication behavior only for new agencies (i.e., if a country's allies develop cyber capabilities within new military agencies, the country is more likely to do the same).

This analysis suggests that neutrality and non-aggression pacts predominantly drive the complementary behavior observed in Table 1. Future research should explore the mechanisms underlying this behavior within these types of alliances.

Discussion and Implications

This research addresses the following question: *How do nations begin developing their cyber capabilities within their militaries?* In particular, *which organizations are established for this task?* The results suggest that allies and bureaucratic politics play a crucial role in this process. Responses to allied behavior create interesting dynamics. On one hand, states may follow their allies by integrating cyber technologies into existing military agencies if their allies have already done so. On the other hand, states might complement their allies' actions by setting up new military agencies to integrate cyber technologies when their allies have started integrating these technologies within existing agencies. While the replication dynamic is somewhat common across all types of alliances, the complementarity dynamic is typically observed only in neutrality and nonaggression pacts. Bureaucratic politics influences the integration process through service dominance: the more equal the distribution of power among military services, the more likely a country is to establish a new agency for integrating cyber technologies.

These findings give rise to several important implications. First, the fact that threats are insufficient in explaining proliferation of cyber capabilities presents a departure from existing scholarship that prioritize threats as one of the main drivers of cybercapabilities (Gomez, 2016; Calderaro and Craig, 2020). It also departs from scholarship that focuses on external threats as one of the primary drivers of military innovations (Posen, 1993;

Waltz, 1979; Resende-Santos, 2007). The transnational nature of cyber-threats and states' digital interconnectedness motivate states to address threats collectively; as a result, the presence or absence of cybercapable allies is one of the drivers of when and how states incorporate cyber technologies. As digital threats continue to expand (with the Internet-of-things, artificial intelligence, and quantum computing), the influence of allies should only become more salient.

Second, my results reinforce prior findings that allies play a role in diffusion of new technologies (e.g., (Kostyuk, 2024)) and add more nuance to this important role. They suggest that not only a membership within a military alliance, but also choices member-states make when integrating new technologies affect a nation's decision when it comes to innovation. States imitate their allies when integrating cyber technologies within their militaries, a pattern observed across all types of alliances. However, only nonaggression and neutrality pacts also exhibit complementarity with their allies' cyber capabilities. Future research should explore the factors driving this complementary behavior among these types of alliances.

The findings enhance our understanding of how countries organize their use of cyber weapons, with significant implications for military innovation, civil-military relations, and military effectiveness. The role of allies and bureaucratic politics in shaping the development of cyber capabilities underscores the importance of international collaboration and internal power dynamics. States aligning their cyber capabilities with those of their allies can benefit from shared expertise and standardized practices, potentially enhancing overall cyber effectiveness. Conversely, the tendency to establish new agencies for cyber capabilities, driven by internal power structures, highlights the influence of bureaucratic politics. While this can lead to more specialized and effective cyber units, it may also introduce additional layers of bureaucracy that could impact agility and coordination. Understanding these dynamics helps policymakers anticipate how cyber technologies will spread and affect operational capacity, such as expecting that countries without a dominant military service are more likely to create new agencies dedicated to cyber threats. This insight is crucial for navigating the complexities of integrating new technologies and managing military organization.

Furthermore, these findings are relevant to the development and integration of other emerging technologies, such as artificial intelligence (AI), which involve broader and more complex considerations beyond specific systems or artifacts. The patterns observed in how states establish and manage cyber capabilities provide valuable insights for approaching AI. For example, the tendency to create specialized agencies for cyber capabilities in response to bureaucratic politics could similarly apply to AI, where dedicated military units might be formed to tackle the unique challenges and opportunities presented by AI technologies. Whether this pattern will emerge with AI remains to be seen, given the relative novelty of these technologies.

A key implication of the study is that new, specialized cyber agencies can enhance operational capacity for cyber missions over the long term. However, integrating cyber capabilities into existing military organizations could offer benefits for combined arms operations, where cyber is used alongside conventional forces. There appears to be a tradeoff between the deep specialization of new cyber organizations and the broader operational integration of cyber capabilities with conventional military assets. While specialized agencies may boost cyber effectiveness, embedding cyber into existing organizations might improve overall operational synergy. This potential tradeoff highlights an important consideration for future research, exploring how cyber integration impacts combined arms operations.

Future research should also focus on the ongoing integration of cyber technologies within militaries. While this article addresses only the initial integration phase, countries typically continue beyond this step. Most nations that initially started developing cyber capabilities within existing military agencies eventually establish new military organizations specifically dedicated to cybersecurity. Additionally, researchers should examine capability beyond military agencies to determine which agencies are prioritized in addressing cybersecurity challenges that often require intergovernmental cooperation. Finally, recent studies highlight the importance of organizational culture in developing cyber strategies (e.g., Kostyuk, Perkoski and Poznansky (2022); Schneider (2024); Lonergan (2024)). Future work should investigate what role organizational culture plays in the establishment of cyber-specific military organizations through detailed case studies.

Much of our current understanding of international politics rests on the assumption that state behavior is shaped by the threat of war and the pursuit of military capability. The empirical study of politics thus depends on how states develop capacity by integrating new technologies, which play a pivotal role in war causation, arms races, alliance formation, conflict duration, or crisis escalation, among others. While this article presents the first comprehensive analysis of how states design their militaries when integrating cyber technologies, future research can add more nuanced explanations of this complex political phenomenon.

References

Allison, Graham T and Frederic A Morris. 1975. "Armaments and arms control: Exploring the determinants of military weapons." *Daedalus* pp. 99–129.

Allison, Graham T and Morton H Halperin. 1972. "Bureaucratic politics: A paradigm and some policy implications." *World politics* 24(S1):40–79.

Berry, Frances Stokes and William D Berry. 1990. "State lottery adoptions as policy innovations: An event history analysis." *American political science review* 84(2):395–415.

Blessing, Jason. 2020. The Diffusion of Cyber Forces: Military Innovation and the Dynamic Implementation of Cyber Force Structure PhD thesis Syracuse University.

Blessing, Jason. 2021. The global spread of cyber forces, 2000–2018. In *2021 13th International Conference on Cyber Conflict (CyCon)*. IEEE pp. 233–255.

Bodea, Cristina and Raymond Hicks. 2015. "Price stability and central bank independence: Discipline, credibility, and democratic institutions." *International Organization* 69(1):35–61.

Borghard, Erica D and Shawn W Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26(3):452–481.

Borghard, Erica D and Shawn W Lonergan. 2019. "Cyber operations as imperfect tools of escalation." *Strategic Studies Quarterly* 13(3):122–145.

Branch, Jordan. 2021. "What's in a Name? Metaphors and Cybersecurity." *International Organization* 75(1):39–70.

Brantly, Aaron Franklin. 2016. *The Decision to Attack: Military and Intelligence Cyber Decision-making*. University of Georgia Press.

Brown, Michael E. 2019. *Flying blind: The politics of the US strategic bomber program*. Cornell University Press.

Buchanan, Ben and Fiona S Cunningham. 2020. "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis (Fall 2020)." *Texas National Security Review* .

Calderaro, Andrea and Anthony JS Craig. 2020. "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building." *Third World Quarterly* 41(6):917–938.

Cunningham, Fiona S. 2022. "Strategic Substitution: China's Search for Coercive Leverage in the Information Age." *International Security* 47(1):46–92.

Dahl, Arden B. 2003. The Warthog. The Best Deal the Air Force Never Wanted. Technical report NATIONAL WAR COLL WASHINGTON DC.

Defence Guidelines for 2025 and Beyond. 2017. Directorate of Defence.

Diehl, Paul F, Gary Goertz and Yahve Gallegos. 2021. "Peace data: Concept, measurement, patterns, and research agenda." *Conflict Management and Peace Science* 38(5):605–624.

Elkins, Zachary, Andrew T Guzman and Beth A Simmons. 2006. "Competing for capital: The diffusion of bilateral investment treaties, 1960–2000." *International organization* 60(4):811–846.

Evangelista, Matthew A. 1984. "Why the Soviets Buy the Weapons They Do." *World Politics* 36(4):597–618.

Fuhrmann, Matthew and Michael C Horowitz. 2017. "Droning on: explaining the proliferation of unmanned aerial vehicles." *International organization* 71(2):397–418.

Gannon, Andres and Nadiya Kostyuk. 2024. "From Bit to Byte: Measuring latent cyber capacity.".

Gannon, Juan Andrés. 2021. *Use Their Force: Interstate Security Alignments and the Distribution of Military Capabilities*. University of California, San Diego.

Gibler, Douglas M. 2008. *International military alliances, 1648-2008*. CQ Press.

Gleditsch, Kristian Skrede and Michael D Ward. 2006. "Diffusion and the international context of democratization." *International organization* 60(4):911–933.

Gomez, Miguel Alberto N. 2016. "Arming Cyberspace: The Militarization of a Virtual Domain." *Global Security and Intelligence Studies* 1(2):5.

Grauer, Ryan. 2015. "Moderating diffusion: Military bureaucratic politics and the implementation of German doctrine in South America, 1885–1914." *World Politics* 67(2):268–312.

Guenther, Lindsey and Paul Musgrave. 2022. "New Questions for an Old Alliance: NATO in Cyberspace and American Public Opinion." *Journal of Global Security Studies* 7(4):ogac024.

Horowitz, Michael C. 2010. *The diffusion of military power: Causes and consequences for international politics*. Princeton University Press.

Huntington, Samuel P. 1961. "Interservice competition and the political roles of the armed services." *American Political Science Review* 55(1):40–52.

Interview. 2018. "Interviews on Cyber Institutions as a Deterrent.".

Jervis, Robert. 1978. "Cooperation under the security dilemma." *World politics* 30(02):167–214.

Jo, Dong-Joon and Erik Gartzke. 2007. "Determinants of nuclear weapons proliferation." *Journal of Conflict Resolution* 51(1):167–194.

Kahn, Lauren and Michael C Horowitz. 2021. "Who Gets Smart: Explaining How Precision Bombs Proliferate." *Journal of Conflict Resolution* .

Kostyuk, Nadiya. 2020. "Deterrence in the Cyber Realm: Public versus private cybercapacity.".

Kostyuk, Nadiya. 2021. "Deterrence in the Cyber Realm: Public versus private cyber capability." *International Studies Quarterly* 28(2):219–238.

Kostyuk, Nadiya. 2022. "Allies & Diffusion of State Military Cybercapacity." *Presented at the American Political Science Association Conference* .

Kostyuk, Nadiya. 2024. "Allies and diffusion of state military cybercapacity." *Journal of Peace Research* p. 00223433241226559.

Kostyuk, Nadiya and Erik A. Gartzke. 2022*a*. "Fighting in Cyberspace: Internet access and the substitutability of cyber and military operations." *Working Manuscript* .

Kostyuk, Nadiya and Erik Gartzke. 2022*b*. "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine (Summer 2022).".

Kostyuk, Nadiya, Evan Perkoski and Michael Poznansky. 2022. "The Sources of Cyber Strategy." *Presented at the International Studies Association Conference* .

Kreps, Sarah and Jacquelyn Schneider. 2019. "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics." *Journal of Cybersecurity* 5(1):tyz007.

Leeds, Brett Ashley. 2005. "Alliance Treaty Obligations and Provisions Dataset." *Rice University (http://www. ruf. rice. edu/~ leeds)* .

Leeds, Brett, Jeffrey Ritter, Sara Mitchell and Andrew Long. 2002. "Alliance treaty obligations and provisions, 1815-1944." *International Interactions* 28(3):237–260.

Liff, Adam P. 2012. "Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war." *Journal of Strategic Studies* 35(3):401–428.

Lindsay, Jon R. 2021. "Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem." *Intelligence and National security* 36(2):260–278.

Lindsay, Jon R and Erik Gartzke. 2015. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." *Typescript, University of California, San Diego* .

Lonergan, Erica D. 2024. "Emerging technology and the cult of the offensive." *Contemporary Security Policy* pp. 1–35.

Lupovici, Amir. 2016. "The "Attribution Problem" and the social construction of "Violence": Taking cyber deterrence literature a step forward." *International Studies Perspectives* 17(3):322–342.

Maoz, Zeev. 2005. "Dyadic Militarized Interstate Disputes Dataset Version 2.0." *UC Davis)* .

Most, Benjamin A, Harvey Starr and Randolph Siverson. 1989. "The logic and study of the diffusion of international conflict." *Handbook of war studies* pp. 111–139.

National Cybersecurity Strategy. 2016. Republic of Bulgaria.

Neufeld, Michael J. 2005. "The end of the Army Space Program: interservice rivalry and the transfer of the von Braun group to NASA, 1958-1959." *The Journal of Military History* 69(3):737–757.

Posen, Barry R. 1993. "Nationalism, the mass army, and military power." *International security* 18(2):80–124.

Resende-Santos, João. 2007. *Neorealism, states, and the modern mass army*. Cambridge University Press.

Rovner, Joshua. 2023. Strategy and Grand Strategy in New Domains. pp. 110–127.

Schneider, Jacquelyn. 2024. "The digital cult of the offensive and the US military." *Journal of Strategic Studies* pp. 1–24.

Simmons, Beth A, Frank Dobbin and Geoffrey Garrett. 2008. "Introduction: the diffusion of liberalization." *The global diffusion of markets and democracy* .

Simmons, Beth A, Paulette Lloyd and Brandon M Stewart. 2018. "The global diffusion of law: Transnational crime and the case of human trafficking." *International organization* 72(2):249–281.

Simmons, Beth A and Zachary Elkins. 2004. "The globalization of liberalization: Policy diffusion in the international political economy." *American political science review* 98(1):171–189.

Siverson, Randolph M and Harvey Starr. 1990. "Opportunity, willingness, and the diffusion of war." *American Political Science Review* 84(1):47–67.

Smeets, Max. 2022. "Cyber Arms Transfer: Meaning, Limits, and Implications." *Security Studies* pp. 1–27.

Tabansky, Lior. 2020. "Israel Defense Forces and National Cyber Defense." *Connections* 19(1):45–62.

Therneau, Terry M and Patricia M Grambsch. 2000. The Cox model. In *Modeling survival data: extending the Cox model*. New York: Springer-Verlag.

U.S. House of Representatives. 2009. "Cybersecurity: A Comprehensive Strategy for Protecting the Nation.". Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security, House of Representatives, 111th Congress, First Session, September 10, 2009.
URL: *https://www.govinfo.gov/content/pkg/CHRG-111hhrg62397/html/CHRG-111hhrg62397.htm*

Valeriano, Brandon, Benjamin Jensen and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.

Walter, Barbara F. 2006. "Building reputation: Why governments fight some separatists but not others." *American Journal of Political Science* 50(2):313–330.

Waltz, Kenneth N. 1979. *Theory of international politics*. Boston, MA: McGraw-Hill.

White, Sarah Payne. 2019. Subcultural Influence on Military Innovation: the Develpment of US Military Cyber Doctrine PhD thesis Harvard University.

Wiener, Craig. 2016. Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation PhD thesis.

Williamson, Oliver E. 1991. "Comparative economic organization: The analysis of discrete structural alternatives." *Administrative science quarterly* pp. 269–296.

Yarhi-Milo, Keren, Alexander Lanoszka and Zack Cooper. 2016. "To arm or to ally? The patron's dilemma and the strategic logic of arms transfers and alliances." *International Security* 41(2):90–139.