How Does Military Professionalization Affect Cyber Capacity Development?

Mustafa Kirisci[1] and Isa Haskologlu[2]
[1]Lebanon Valley College, USA
[2]American University, USA

kirisci@lvc.edu
haskolog@american.edu

Abstract: This paper investigates how military professionalization influences a state's propensity to incorporate cybersecurity responsibilities within their militaries. We argue that states with more professional militaries would be more likely to initiate cyber-capacity development. Employing quantitative analysis, this study analyzes cross-national data to test the hypothesis that states with higher levels of military professionalization are more likely to initiate the development of military cyber capacities. Our empirical results support this hypothesis, demonstrating a significant positive correlation between the degree of military professionalization and the likelihood of adopting new cybersecurity responsibilities. Our results also offer explanation as to which dimensions of professionalization are more strongly related to the adoption of military cyber capabilities.

Keywords: Cyber-capacity, Development, Initiation, Military, Professionalization

1. Introduction

In recent years, Germany—with one of the most professionalized militaries in Europe—has emerged as a leader in military cyber capacity development. In 2017, Germany launched its Cyber and Information Space Command (CIR), marking a significant shift in its defense strategy to include cyber warfare capabilities. This development was driven by the professionalization of Germany's military, which emphasizes specialized training, strategic coordination, and close military-civilian collaboration in cybersecurity. In contrast, Nigeria, despite facing growing cyber threats, has struggled to establish significant military cyber capacity. The Nigerian military, which lacks the structured professionalization found in Germany's forces, has been slow to adopt cyber capabilities, largely due to organizational weaknesses, a lack of specialized training, and an over-reliance on external support for cybersecurity. These contrasting cases raise a crucial research question: How does military professionalization affect a nation's ability to develop military cyber capacity?

The existing literature on military cyber capacity development has largely focused on technology, resources, and geopolitical factors (Libicki, 2017; Valeriano & Maness, 2015). Much of the research emphasizes the importance of technological infrastructure and state-sponsored investments in cyber tools, while others highlight the influence of international cooperation on enhancing cyber capabilities (Bendiek, 2018). However, military professionalization—the processes of formal education, hierarchical structure, and personnel specialization within the armed forces—has not been given due attention. In countries like Germany, professionalized military forces have enabled a structured, proactive approach to cyber defense. This contrasts sharply with less professionalized militaries, where cyber capacity either remains underdeveloped or is outsourced to civilian agencies or private contractors, as seen in Nigeria's case.

This research fills the gap in existing literature by introducing military professionalization as a critical factor in cyber capacity development. By studying how well-trained, structured, and specialized military forces can influence a nation's cyber readiness, we offer a new perspective on cyber capacity building. Countries with highly professionalized militaries are better positioned to integrate cybersecurity into their defense strategies, while nations with under-professionalized forces often struggle with fragmented or inadequate cyber capabilities. Understanding these dynamics is crucial in a world where cyber warfare is increasingly part of national defense.

Our contribution highlights that, while technological development and funding are important, military professionalization can be the determining factor in whether a country successfully develops military cyber capacity. This approach underscores the importance of the human and organizational dimension of cybersecurity, providing insights into how countries with varying levels of military professionalism approach cyber defense. Without professionalization, even the most well-funded military organizations may lack the coordination and strategic foresight to effectively handle cyber threats.

2. Overview of Existing Literature

Kostyuk (2024) defines state military cybercapacity as "ability of a nation-state's military to effectively conduct operations in cyberspace, including defense of its own networks and systems from cyber-threats and execution of offensive cyber-operations for various purposes, including intelligence gathering and disruption of adversarial networks."(Kostyuk, 2024, p. 46)

With the developments in the cyber realm, it is very critical for a state to ability to defend itself in the cyberspace, defend against and respond to cyber threats. As Langø (2016) argues, cyber capacity building is not only a risk management endeavor, it is also an essential component of the intersection of technology and politics. Developments in the international and communication technology are multifaceted and can easily undermine the trust between the government and the people. Thus, governments should comprehensively approach and address their cyber capacity building processes. Building a cyber capacity requires a comprehensive approach as it requires legal, institutional, social, governance in addition to following the latest developments in technology.

Threatening security environment

Another factor that pushes countries' cyber readiness is their environment. Countries with more hostile security setting are expected to have higher level of cyber capacity (Christos Makridis et al., 2019). On the other hand, Kostyuk (Kostyuk, 2024) argues that threat environment and security dilemma fails to explain the military cyber capacity building thoroughly as states face similar cyber threats do not take similar measures and build similar military cyber capabilities.

Difference Between The Developed and Developing Nations.

The cyber capacity among states vary, especially between developed and developing nations (Pawlak & Barmpaliou, 2017). Developing countries lack of access to latest technology, required infrastructure, and experts to apply cybersecurity measures (Muller, 2015). Moreover, developing countries have fragile governance structures and insufficient institutional capacity as well as limited resources, human resource, and institutional reforms to implement an effective cyber capacity building (Muller, 2015). Developing countries can build and maintain their cyber capacity if they benefit from the experiences of countries with successful cyber capacity and get support of the international organizations such as United Nations and International Telecommunication Union. Schia (2018) argues that the developing countries can increase their cyber capacity by investing in digital infrastructure while promoting digital literacy.

Yet, building and investing in a cyber capability is quite costly (Perlroth, 2021). Developed nations on the other hand, can invest in large amounts of its resources to build and maintain an effective cyber capacity. In 2011, the UK allocated £650 million to cyber capacity building (Pace & Cornish, 2021). The UK has also kickstarted the Global Conference on Cyberspace. Following the UK, several other developed countries like Japan, Estonia, Singapore, and Australia have started their cyber programs. One other factor that defines a countries' cyber capacity level is their science and technical knowledge (Calderaro & Craig, 2020).

On the other hand, Makridis et al. (Calderaro & Craig, 2020) argue that there is not a statistically significant relationship between institutional capacity and cyber readiness. Resource capacity does not have a significant impact on the cyber readiness.

Role of international community and Alliances

Cybersecurity capacity building around the world is largely ungoverned, unsystematic, and fragmented, an environment with a flood of enterprises and interventions which cause repetition of efforts and overspending (Pace & Cornish, 2021). Besides, this environment provides safe havens for cyber criminals. Many national actors have similar vulnerabilities that can be exploited by the attackers simultaneously or in succession as seen in the example of the malicious code found in Ukrainian power grids and soon after in the U.S. system (Koehler, 2018). As mutual vulnerability is a key feature of cybersecurity among member states, harmonization and coordination of efforts is a required component to build an effective and efficient national cyber capacity. In this environment, international organizations and formal alliances such as the UN, the EU, NATO, and OECD play a crucial role in diffusion of national cybersecurity strategies, setting norms and standards for cybersecurity, in providing technical assistance, training and capacity-building programs (Kostyuk & Sidorova, 2024).

As Kostyuk (2024) argues, country's alliances have a significant impact on its cyber capacity building process (Kostyuk, 2024). Powerful alliance members can share their military cyber capabilities with weaker members to increase coalition's overall security (Yarhi-Milo et al., 2016). Strong members can also help weaker members to build their own capability without sharing their capabilities (Kostyuk, 2024).

States not only use their resources to build a cyber capacity, but also participate in multilateral efforts to improve their capacity (Watanabe, 2020). National governments are willing to contribute to the international cyber capacity building measures. For example, in 2016, Singapore declared 10 million USD fund for cyber capacity building among the ASEAN member states (Pace & Cornish, 2021). In 2019, Singapore pioneered the establishment of a regional cyber capacity building center. Regional organizations conduct cyber trainings, drill exercises, and knowledge share to increase awareness and provide cyber readiness of nation states. Organized cyber exercises and drills conducted by The Organization of American States (OAS), International Telecommunication Union (ITU), and the International Multilateral Partnership Against Cyber Threats (IMPACT) is of one example (Muller, 2015). Yet, nation states' degree of political will makes a big impact on implementing and maintaining their cyber capacity. Estonia is one example. It has spent and invest in building its cyber capacity as it was worried concerned that major NATO allies might not offer a sufficient support in the event of a cyber-attack(Kostyuk, 2024). Besides, one-size-fits all solutions may not be enough to build cyber capacity for every nation state as countries might have different interests, priorities, and resources.

3. Theoretical Framework

Conceptualizing Military Professionalization and Military Cyber Capacity Development

Military professionalization refers to the formal structuring, training, and educational processes that create skilled, hierarchical, and specialized military forces. In professionalized militaries, strategic approaches to defense—including modern warfare techniques and innovations—are prioritized. The works of Huntington (1957) and Janowitz (1960) have extensively outlined the role of military professionalism in enhancing the complexity and sophistication of military operations.

Military cyber capacity development refers to the establishment of dedicated cyber units, cyber defense strategies, and cybersecurity roles within military institutions. The rapid rise of cyber warfare as a key threat to national security has made cyber capacity essential for modern militaries (Libicki, 2017; Valeriano & Maness, 2015). Military cyber capacity involves the protection of critical infrastructure, the ability to engage in cyber operations, and ensuring national cyber sovereignty (Bendiek, 2018). Countries with professionalized militaries are better equipped to initiate such capabilities.

4. How Military Professionalization Increases the Likelihood of Cyber Capacity Initiation

The link between military professionalization and the initiation of military cyber capacity can be explained through several mechanisms:

- Higher Military Expenditure and Investment in Advanced Technologies

Professionalized militaries tend to have greater financial resources allocated toward developing defense technologies, including cyber tools (Dunn Cavelty, 2013). Countries with high levels of military professionalization generally have the budgetary flexibility to invest in the necessary digital infrastructure and create specialized cyber units. For instance, Germany's creation of its Cyber and Information Space Command (CIR) in 2017 was supported by years of military modernization (Bendiek & Porter, 2019).

In contrast, Venezuela in South America and Yemen in the Middle East, which both have under-professionalized militaries, struggle to develop robust cyber capabilities due to limited resources and inconsistent military investments. Venezuela's military has faced budget constraints amid ongoing economic crises, leading to an inability to prioritize cyber defense development (Trinkunas, 2014). Similarly, Yemen's military, plagued by years of conflict and organizational disarray, lacks the resources and infrastructure to develop effective cyber capabilities (Watson, 2021).

- Access to Expertise and Intellectual Resources

Professionalized militaries benefit from robust intellectual ecosystems that support continuous education, research, and strategic adaptation. Military academies, research institutions, and defense-related think tanks provide the intellectual foundation for cyber innovation (Biddle, 2006). For example, countries like Germany

and the United States have used their military academies and research centers to produce cybersecurity experts who can lead the development of military cyber capacity (Geiss & Lahmann, 2020).

By contrast, Uganda in East Africa and Bangladesh in South Asia have militaries that lack these intellectual resources. Uganda's military has focused on conventional warfare strategies with limited attention to developing cyber expertise, reflecting the absence of dedicated military education on cybersecurity (Turyasingura, 2020). Similarly, Bangladesh's military has relied heavily on civilian-led cyber initiatives and has not developed a strong military cyber education framework, leaving its defense forces ill-equipped to address cyber threats independently (Chowdhury, 2020).

- Organizational Responsiveness and Adaptation to Emerging Threats

Professionalized militaries demonstrate a higher capacity to adapt to emerging threats, including cyberattacks, through structured processes and strategic coordination. Their ability to identify and respond to new security challenges is a hallmark of their professionalism (Kuehl, 2009). For example, the U.S. military's creation of U.S. Cyber Command in 2009 illustrates how professionalized forces can quickly organize to confront cyber threats (Lindsay, 2015).

In contrast, Honduras in Central America and Pakistan in South Asia have under-professionalized militaries that struggle with bureaucratic inefficiencies and lack the organizational structures needed to respond to cyber threats effectively. Honduras has limited military capabilities in the cyber domain and has been slow to address the growing threat of cyberattacks due to a lack of strategic focus on cyber defense (Gomez, 2020). Similarly, while Pakistan has acknowledged the importance of cyber defense, its military remains under-organized in this regard, with cyber operations largely managed by civilian entities, reflecting the country's struggles with military professionalism (Khan, 2019). We conclude this section with our hypothesis.

Hypothesis: Higher levels of military professionalization are positively associated with a higher likelihood of initiating military cyber capacity development.

5. Research Design

We use time series cross sectional data to test our hypothesis. Because we examine countries' behavior in different years in terms of their military professionalization efforts and military cyber capacity development, our unit of analysis is country-year. Our data covers the period of 2000-2018, and includes 738 country-year observations.

Our dependent variable is whether a country includes a new cybersecurity responsibility to its Ministry of Defense/Department of Defense in a given year. If the country included such a responsibility in a given year between 2000 to 2018, it is coded 1 in the dataset and the country didn't add such a responsibility in a given year, it is coded 0. Because we use a binary dependent variable, our estimation method will be logistic regression. We measure the dependent variable with State Cybersecurity Organizations Data (v.1.0). The original data developed by Nadiya Kostyuk includes the time coverage from 1988 to 2018, but the entire data is not publicly released yet, so we use the replication data set of Kostyuk's (2024) article that uses certain portion of this data. And this replication data's time coverage is 2000-2018.

Some scholars use publicly attributed cyber operations as a measure of state military cyber capacity (e.g., CSIS Significant Cyber Incidents Data), but this approach has limitations (Kostyuk, 2024): since cyber operations depend on secrecy to succeed, attributed operations could signal failure, and successful covert operations may remain unknown, potentially misrepresenting state capacity (Gartzke & Lindsay, 2015). Others use institutions as indicators of military capability (Early, 2014; Fuhrmann & Horowitz, 2017; Kostyuk, 2021), yet institutional presence doesn't always align with actual capacity, as seen with military cyber commands that may lack operational ability despite high investment (Smeets, 2022). Consequently, we use Kostyuk's measure of initiation of military cyber capacity development. To illustrate the distribution of military cyber capacity development across different regions of the world, Kostyuk (2024) provides the following figure (i.e. Figure 1) that shows instances when countries from different regions of the world began developing their military cyber capacity.

Our independent variable is the levels of professionalization of militaries of countries included in the data in the period of 2000-2018. When measuring military professionalism across many countries over an extended period, researchers often face a trade-off between data accuracy and availability (Toronto, 2017). Detailed data on military development are obtainable for select countries (Pascal et al., 1979; Beattie, 2001), but such data collection is often too costly or impractical for large datasets covering many countries and years. To

address this, this study borrows three indicators from Toronto's (2017) military professionalization data, which balance accuracy with feasibility: military expenditures per soldier, the number of military academies, and military periodicals. While these indicators may lack precision for all cases over time, they offer a practical approach for assessing institutionalized military professionalism (Toronto, 2017).

As per the military expenditure per soldier measure, a country that dedicates more resources per soldier is likely to have better trained and better educated officers corps, and that suggests a greater level of expertise in both officer and enlisted ranks (Toronto, 2017). Higher military spending per soldier is often linked to greater investment in advanced training, technology, and specialized resources, enabling the development of sophisticated capabilities like military cyber operations, which require significant technical infrastructure and expertise. Toronto (2017) obtains this measure by using the Correlates of War Project's (2010) National Material Capabilities (NMC) data set, version 4.0, which provides country-year observations from 1816 to 2007 (Singer, Bremer, and Stuckey 1972, 1987). He divides the NMC's military expenditure variable by the active-duty military personnel to arrive at the military expenditure per soldier variable (Toronto, 2017, 859).

In terms of the number of military academies measure, military academies focus on educating future officers in the skills and knowledge they will need to perform their duties (Toronto, 2017). Having more military academies is associated with a higher chance of initiating military cyber capacity development because these institutions foster specialized training and research, building a workforce with the technical and strategic skills necessary for cyber operations. In Toronto's (2017) data, "the observations regarding military academies are individual military schools, with information on which state the school is located in, the years the school has been or was in operation, whether it meets the criteria for being a military academy (being controlled by the state and graduating cadets to commissions), and the sources used to support the observation." (Online Codebook, p.2). Toronto (2017) relies on individual states' Ministry of Defense and armed forces websites, the websites of military schools, and a wide array of secondary historical sources in coding the military academies data. The time coverage of the observations on the number of military academies is from 1816 to 2005.

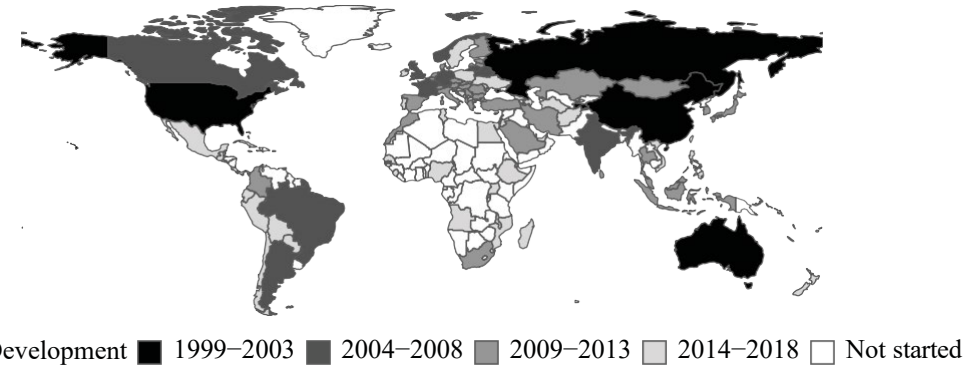
The final indicator of military professionalization is military periodicals. Military periodicals provide a platform for sharing and developing knowledge on managing conflict, so a higher number of these publications suggests a wider and more diverse expertise within the officer corps (Toronto, 2017, p.860). A high number of military periodicals is associated with a greater chance of initiating military cyber capacity development because these publications facilitate the exchange of specialized knowledge, enabling military professionals to stay informed about emerging threats and technological advances like cyber warfare. By fostering an environment of continuous learning and debate on security innovations, periodicals help cultivate an officer corps that is both aware of and prepared to advocate for cyber capabilities as part of national defense. The observations of the count of military periodicals data included in Toronto's (2017) data set are individual military periodicals. And these observations include "information on the country and years of publication, as well as any other names by which the periodical has been known . "Almost all observations come from two sources: Ulrich's Periodicals Directory (2005) and WorldCat (FirstSearch 2005), and the oldest periodical appears in this data set in 1796, and observations run through 2005". (Online Codebook, p.2). In our data, because the number of military periodicals range from 0 to 199 and has a high standard deviation, we take the natural log of this variable in our models.

By using these three variables, we create an index that captures the concept of military professionalization. We run Cronbach alpha analysis to see if this index empirically captures the military professionalization concept. Our Cronbach alpha shows 0.7020, which is acceptable and confirms that our index captures the concept we intended to measure. We also run a factor analysis to see how much each variable contributes to the military professionalization concept. The findings of the factor analysis are demonstrated in the appendix due to word count constraints. The number of observations shows lower than 738 due to missing data on the number of military academies variable.

Table 1: Descriptive Statistics

Variable	Obs	Mean	Std.Dev.	Min	Max
Military cyber capacity initiation	2526	.036	.187	0	1
Military professionalization index	472	.184	.787	-1.256	3.615
Number of military academies	493	1.282	1.342	0	10
Number of military periodicals	738	6.362	18.938	0	199

Variable	Obs	Mean	Std.Dev.	Min	Max
Military expenditure per soldier	696	9.474	1.417	5.809	12.658
Membership in military IGOs	2526	0	1	-3.247	3.656
Adversary cyber capacity initiation	2526	.049	.215	0	1
Democracy	2526	.52	.5	0	1
GDP per capita	2526	0	1	-2.108	2.47
Number of internet users	2526	0	1	-1.816	1.625



Source: State Cybersecurity Organizations Data (v1.0), collected by Kostyuk (2024).

Figure 1: Initiation of the military cybercapacity development (1999–2018)

Before concluding this section, we also discuss the control variables that may confound the relationship between military professionalization and the likelihood of initiating military cyber capacity development. To this end, we control for several factors. First, we control for democracies because civilian in democracies, oversight and transparency requirements can shape military objectives, prioritize ethical considerations, and facilitate technological investments. Democracies also tend to support institutional development, which can affect both professionalization and cybersecurity readiness through structured training, adherence to doctrines, and systematic innovation. Marshall, Gurr and Jagger's (2019)'s Polity IV score is used to create a dummy variable that takes the value of a 0 if this score is less than 6 representing an autocracy, and 1, if this score is more than equal to 6 representing a democracy (Kostyuk, 2024). Membership in intergovernmental organizations (IGOs) whose primarily focus is peace, defense and security is also controlled as being a member to these sorts of IGOs would allow states to interact with states that already started to develop military cyber capacity, and that interaction would increase the chances of a state to start their own military cyber capacity development. Pevehouse et al.'s (2020) (Membership in Military IGOs) dataset is used to measure military IGO membership and the scores of this variable is weighted.

Adversaries' cyber capacity initiation prior to the decision to start a state's own cyber capacity is also controlled in order to capture threat perception of countries. This measure of whether adversaries developed cyber capacity is borrowed from Kostyuk (2024). Kostyuk (2024) identified the adversaries from Maoz's (2005) data on Militarized Interstate Disputes (MID) and Valeriano et al.'s (2018) Dyadic Cyber Incident Dataset (DCID) (v1.5). We also account for material resources of countries, which is captured by GDP per capita from World Bank data. Finally, the number of internet users is also controlled as it can be indicative of a country's overall access to digital infrastructure and technological resources. Higher internet usage may correlate with more developed cyber capabilities, which can influence military cyber capacity development. This variable is also measured with World Bank data, and both GDP per capita and the number of internet user variables are logged.

6. Results

In Table 2, we present the results of the logistic regression. We use STATA to conduct our quantitative analyses. The positive coefficients represent positive relationship between a given variable and the dependent variable, and the negative coefficients suggest the otherwise. The coefficients with stars represent statistical significance. One star represents statistical significance at 90 percent confidence interval, 2 stars represent 95 percent confidence interval, and 3 stars represent 99 percent confidence interval. We present four models.

The first model includes the indexed military professionalization variable and control variables. The later models include one of the indicators of military professionalization and all other controls.

The results in the table suggest that the military professionalization variable has a positive coefficient in the first model and it is statistically significant at 95 percent confidence interval (p-value is 0.012). The number of military academies variable has a statistically insignificant coefficient, suggesting that it does not significantly affect the likelihood of military cyber capacity development. As per the other indicators of military professionalization, both number of military periodicals and military expenditure per soldier variables have positive and significant coefficients at 99 percent and 95 percent confidence intervals, respectively (p values are 0.001 and 0.029, respectively). These findings suggest that greater number of periodicals and military spending per soldier are associated with higher chance of initiating military cyber capacity development. In terms of the control variables, the adversaries' cyber capacity development variable's coefficients are statistically significant and large in size across all models. They all have positive signs, suggesting that adversaries' cyber capacity development has a strong and significant impact on the state's decision to develop its own military cyber capacity. Military IGO membership, democracy and number of internet users have all insignificant coefficients across all models. This shows these variables do not significantly affect the probability of initiating military cyber capacity development. The findings about GDP per capita are mixed. Its coefficients achieve statistical significance in the first and the last models with negative signs, but not in the second and third model. This indicates this variable has a mixed effect on the chance of military cyber capacity development.

In addition to the main models, we also run a robustness check analysis with rare event logit as only 3.64 percent of the observations report initiation of military cyber capacity development. In Table 3, we present the findings of the rare event logit analysis, and our main findings are consistent with the ones in the main models in terms of statistical significance and the signs of the coefficients of the independent variables.

Table 2: Logistic Regression Analysis of Military Cyber Capacity Development

	(Model 1)	(Model 2)	(Model 3)	(Model 4)
VARIABLES				
Military professionalization(index)	1.297**			
	(0.517)			
Number of military academies		-0.0196		
		(0.298)		
Number of military periodicals (logged)			1.179***	
			(0.341)	
Military expenditure per soldier				1.503**
				(0.526)
Adversaries' cyber capacity development	2.785**	2.992***	2.373**	3.317**
	(1.167)	(1.102)	(1.041)	(1.325)
Military IGO membership	0.458	0.544	0.393	0.310
	(0.870)	(0.792)	(0.647)	(0.558)
Democracy	0.999	1.501	0.601	1.463
	(1.222)	(1.221)	(0.593)	(0.163)
GDP per capita (logged)	-1.324**	-0.777	-1.083	-1.965***
	(0.672)	(0.662)	(0.668)	(0.642)
Number of internet users (logged)	0.00781	0.119	-0.0603	0.169
	(1.210)	(1.021)	(0.928)	(1.228)
Constant	-6.105***	-5.776***	-7.880***	-19.60***
	(1.752)	(1.492)	(1.564)	(5.931)

	(Model 1)	(Model 2)	(Model 3)	(Model 4)
Observations	472	493	738	696

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 3: Rare Event Logit Analysis of Military Cyber Capacity Initiation

	(Model 1)	(Model 2)	(Model 3)	(Model 4)
VARIABLES				
Military professionalization index	1.211**			
	(0.485)			
Number of military academies		0.120		
		(0.313)		
Number of military periodicals (logged)			1.029***	
			(0.350)	
Military expenditure per soldier				1.325**
				(0.536)
Adversaries' cyber capacity initiation	2.628**	2.865***	2.273***	
	(1.077)	(1.027)	(0.882)	
Military IGO membership	0.453	0.545	0.387	
	(0.862)	(0.781)	(0.636)	
Democracy	0.755	1.129	0.499	0.838
	(1.245)	(1.218)	(0.750)	(0.898)
GDP per capita (logged)	-1.102	-0.542	-0.976	-1.904***
	(0.700)	(0.648)	(0.666)	(0.486)
Number of internet users (logged)	-0.0423	0.00176	-0.00531	0.537
	(1.209)	(0.993)	(0.951)	(0.710)
Constant	-5.263***	-5.123***	-6.799***	-18.03***
	(1.731)	(1.481)	(1.584)	(5.971)
Observations	472	493	738	696

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Beyond the logistic regression analyses, we also show the substantive effects of the independent variables by using "CLARIFY" package in STATA. We report the changes in the probability of initiating military cyber capacity development for different scores of the independent variables. As shown in Tables 4, 5 and 6, as the level of military professionalization, military spending per soldier as well as the number of military periodicals increase, the likelihood of initiating military cyber capacity development shows a substantial increase, as evidenced by the reported percentage changes in the probabilities.

Table 4: The Substantive Effects of Military Professionalization on Initiating Military Cyber Capacity Development

The scores of military professionalization index	Probability of initiating military cyber capacity development	Percentage change in the probability of initiating military cyber capacity development
-1	0.00161	-1 to 0: +180.7%
0	0.00452	0 to 1: +258.4%
1	0.0162	1 to 2: +303.1%
2	0.0653	2 to 3: +205.7%
3	0.1996	-

Table 5: The Substantive Effects of Military Periodicals on Initiating Military Cyber Capacity Development

The logged score of number of military periodicals	Probability of initiating military cyber capacity development	Percentage change in the probability of initiating military cyber capacity development
0	.0009	0 to 1:+155%
1	.0023	1 to 2: +204.3%
2	.0070	2 to 3: +232.9%
3	.0233	3 to 4: +233%
4	.0776	4 to 5: 161.2%
5	.2027	-

Table 6: The Substantive Effects of Military Periodicals on Initiating Military Cyber Capacity Development

The score of military expenditure per soldier	Probability of initiating military cyber capacity development	Percentage change in the probability of initiating military cyber capacity development
5	.00051	5 to 7: - 11.7%
7	.00045	7 to 9: +160%
9	.00117	9 to 11: +1000.57%
11	.01354	-

7. Conclusion

In this research, we examine how military professionalization influences states' decision to initiate military cyber capacity development. We argue that states with more professionalized militaries are more likely to add cyber responsibilities to their militaries. Our quantitative analysis provides strong support for this hypothesis as the findings are significant across different models and robust to different model specification. The substantive effects of our independent variables are also strong, suggesting that every additional increase in military professionalization efforts could substantially increase the chance of initiating military cyber capacity development. The only limitation on our findings is the findings about the number of military academies. In fact, the findings about this variable are actually not surprising, given that it doesn't contribute significantly to the military professionalization index, as evidenced in factor loading analysis.

The empirical findings of this research provide some implications for the existing literature. First, while the external threats play a significant role in explaining state decision to develop new cyber capabilities, these findings highlight the importance of professionalization of the organizations to these state decisions. The findings show that spending more per soldier and documentation and dissemination of military knowledge and experience in periodicals would make militaries be more ready to take on the cyber responsibilities, thereby encouraging policymakers to add cyber responsibilities to their militaries. Second, although we focused on three particular indicators of military professionalization and two of them are highly significant in explaining the decision to initiate military cyber capacity development, the future research may focus on the role of different indicators of military professionalization, which could help the scholar studying on cybersecurity and cyberwarfare to further explore how military professionalization affects state behaviors when it comes to adding new cyber capabilities to militaries.

Third, another future research recommendation is to use updated datasets to examine military professionalization and the development of military cyber capabilities. Using more recent datasets on these key variables would help scholars to explain the relationship between two variables for a longer time range. Furthermore, using more recent datasets would offer a stronger explanatory power to the empirical findings. Fourth, our study focuses on how military professionalization affects the development of cyber forces of countries. As a follow up project, future research would seek explanations for how these military cyber forces are used by countries in different contexts, such as during cyber conflict.

References

Andress, J., & Winterfeld, S., 2013. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Syngress.
Beattie, P.M., 2001. The Tribute of Blood: Army, Honor, Race, and Nation in Brazil, 1864–1945. Durham, NC: Duke University Press.
Bendiek, A., 2018. The EU's cyber capacity building in developing countries: A strategy under construction. European Union Institute for Security Studies.
Bendiek, A., & Porter, H., 2019. Military cyber defense strategies in Germany and the United States. Comparative Strategy, 38(4), pp.312–328.
Bendiek, A., 2012. European cyber security policy. SWP Research Paper, No. RP 13/2012.
Biddle, S., 2006. Military Power: Explaining Victory and Defeat in Modern Battle. Princeton University Press.
Calderaro, A., & Craig, A.J., 2020. Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. Third World Quarterly, 41(6), pp.917–938.
Chowdhury, A.R., 2020. Bangladesh's approach to cybersecurity: Between civilian and military control. South Asian Defense Review, 2(1), pp.12–25.
Dunn Cavelty, M., 2013. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
Early, B.R., 2014. Exploring the final frontier: An empirical analysis of global civil space proliferation. International Studies Quarterly, 58(1), pp.55–67.
Fuhrmann, M., & Horowitz, M.C., 2017. Droning on: Explaining the proliferation of unmanned aerial vehicles. International Organization, 71(2), pp.397–418.
Gartzke, E., & Lindsay, J.R., 2015. Weaving tangled webs: Offense, defense, and deception in cyberspace. Security Studies, 24(2), pp.316–348.
Geiss, R., & Lahmann, H., 2020. Germany's cybersecurity strategy: Military and civilian approaches. Journal of Cybersecurity Studies, 4(2), pp.45–63.
Gomez, J., 2020. Cybersecurity challenges in Honduras: A path to strengthening defense. Latin American Cybersecurity Journal, 6(3), pp.23–35.
Hans-Inge Giske Langø, & Langø, H.-I.G., 2016. Cyber security capacity building: Security and freedom.
Huntington, S.P., 1957. The Soldier and the State: The Theory and Politics of Civil-Military Relations. Harvard University Press.
Janowitz, M., 1960. The Professional Soldier: A Social and Political Portrait. The Free Press.
Khan, I., 2019. Pakistan's cybersecurity preparedness: A realist assessment. Journal of Defense Studies, 13(4), pp.75–92.
Koehler, R.K., 2018. When the lights go out: Vulnerabilities to US critical infrastructure, the Russian cyber threat, and a new way forward. Georgetown Secur. Stud. Rev., 7(1), pp.27–36.
Kostyuk, N., 2021. Deterrence in the cyber realm: Public versus private cyber capacity. International Studies Quarterly.
Kostyuk, N., 2024. Allies and diffusion of state military cyber capacity. Journal of Peace Research, 61, pp.44–58.
Kostyuk, N., & Sidorova, J., 2024. Role of international organizations and formal alliances in the global diffusion of national cybersecurity strategies.
Kuehl, D.T., 2009. From cyberspace to cyberpower: Defining the problem. In F.D. Kramer, S.H. Starr & L.K. Wentz, eds., Cyberpower and National Security. Potomac Books.
Libicki, M.C., 2017. Cyberdeterrence and Cyberwar. RAND Corporation.
Libicki, M., 2021. Cyberspace in Peace and War. Naval Institute Press.
Lindsay, J.R., 2015. Tipping the scales: The digital revolution and the future of cyber warfare. Oxford University Press.
Maoz, Z., 2005. Dyadic Militarized Interstate Disputes Dataset Version 2.0. University of California Davis.
Marshall, M.G., Gurr, T.R., & Jaggers, K., 2019. Polity IV Project: Political Regime Characteristics and Transitions, 1800–2018. Center for Systemic Peace.
Muller, L.P., 2015. Cyber security capacity building in developing countries: Challenges and opportunities.
Olaniyan, D.A., 2018. Cybersecurity in Nigeria: Challenges and prospects. African Security Review, 27(2), pp.106–121.
Pace, L., & Cornish, P., 2021. Cybersecurity capacity building. In The Oxford Handbook of Cyber Security, pp.463.
Pascal, A.H., Kennedy, M., & Rosen, S.P., 1979. Men and Arms in the Middle East: The Human Factor in Military Modernization. RAND Corporation.
Pawlak, P., & Barmpaliou, P.-N., 2017. Politics of cybersecurity capacity building: Conundrum and opportunity. Journal of Cyber Policy, 2(1), pp.123–144.
Pevehouse, J.C., Nordstrom, T., McManus, R.W., et al., 2020. Tracking organizations in the world: The Correlates of War IGO Version 3.0 datasets. Journal of Peace Research, 57(3), pp.492–503.
Perlroth, N., 2021. This is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury Publishing USA.

Schia, N.N., 2018. The cyber frontier and digital pitfalls in the Global South. Third World Quarterly, 39(5), pp.821–837.
Smeets, M., 2022. No Shortcuts: Why States Struggle to Develop a Military Cyber-Force. London: Hurst.
Trinkunas, H., 2014. Venezuela's enduring political-military crisis. Brookings Institution.
Turyasingura, R., 2020. Cybersecurity readiness in Uganda: The role of the military in national defense. African Journal of Cybersecurity Studies, 5(1), pp.14–29.
Valeriano, B., Jensen, B., & Maness, R.C., 2018. Cyber Strategy: The Evolving Character of Power and Coercion. Oxford University Press.
Valeriano, B., & Maness, R.C., 2015. Cyber War Versus Cyber Realities: Cyber Conflict in the International System. Oxford University Press.
Watanabe, S., 2020. Strategic analysis of capacity building for the cyber security of the United States in Asia. Jurnal Asia Pacific Studies, 4(2), pp.100–111.
Watson, E., 2021. Yemen's military fragmentation and its impact on national security. Middle East Defense Journal, 15(2), pp.89–101.
Yarhi-Milo, K., Lanoszka, A., & Cooper, Z., 2016. To arm or to ally? The patron's dilemma and the strategic logic of arms transfers and alliances. International Security, 41(2), pp.90–139.