'Cyber Chess: Using a New Panel Dataset to Identify Global Patterns in National Cybersecurity-Strategy Adoption'

Research Note[*]

Nadiya Kostyuk[†] and Jen Sidorova[‡]

November 11, 2025

Abstract

Over the past two decades, nearly one hundred countries have adopted their first national cybersecurity strategies; however, the timing of these adoptions varies significantly. While a notable increase occurred after 2010, the catalysts behind this surge and the broader motivations driving countries to establish such strategies remain subjects of debate. Existing studies present conflicting arguments, drawing from diverse evidence and often focusing narrowly on specific countries or limited comparative analyses. This study addresses these debates by assembling the first comprehensive dataset, the National Cybersecurity Strategies (NCS) data, which covers the adoption of national cybersecurity strategies by 193 countries from 2000 to 2024. Our findings highlight the pivotal role of international-organization membership—and, to a lesser extent, military alliances and the cyber-threat environment—in driving

[*]We would like to thank Andres Gannon, Ryan Shandler, Brandon Valeriano, and the participants of the 23rd Workshop on the Economics of Information Security. The earlier version of this paper was presented at the 2023 and 2024 International Studies Association Conferences and at the 2023 Association for Public Policy Analysis and Management Conference. Replication materials for this article are available on the ISQ Dataverse at https://dataverse.harvard.edu/dataverse/isq. All the questions regarding replication should be directed to kostyuk.nadiya@gmail.com.

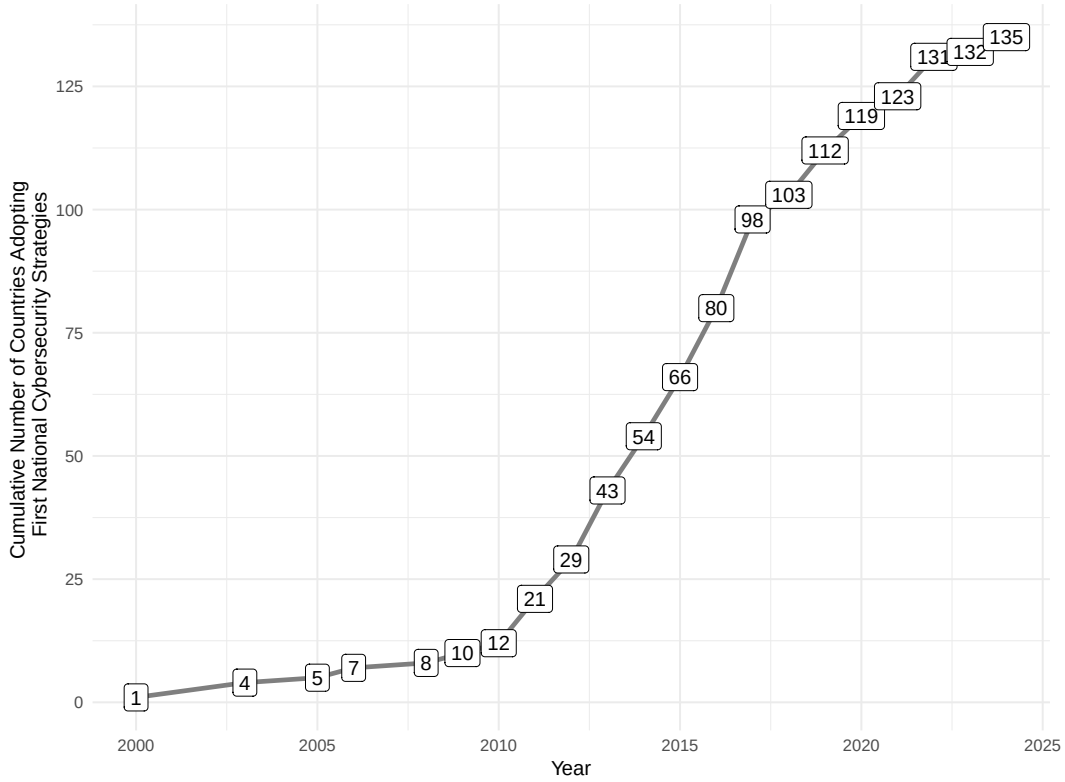
[†]Assistant Professor, Carnegie Mellon Institute for Strategy and Technology, Carnegie Mellon University; nkostyuk@andrew.cmu.edu

[‡]PhD candidate, School of Public Policy, Georgia Institute of Technology; esidorova3@gatech.edu

adoptions. The NCS dataset not only equips researchers and policymakers with a valuable tool to study national cybersecurity strategies but also provides broader insights into the dynamics of policy diffusion across diverse issues, facilitating inquiry into broader international-relations questions.

Over the last two decades, almost a hundred countries adopted their first national cybersecurity strategies. However, their adoption pattern is not linear. Following the lead of Russia in 2000 and Norway and the U.S. in 2003, twelve countries adopted their first national cybersecurity strategies between 2000 and 2010, and an additional 123 nations did so between 2011 and 2024 (Figure 1). The notable post-2010 surge prompts intriguing questions: *What factors triggered the sharp increase after 2010?* More broadly, *when and why does a country decide to adopt its first national cybersecurity strategy, and why do some nations lead and some lag behind in this process?*

Figure 1: ADOPTION OF FIRST NATIONAL CYBERSECURITY STRATEGIES (2000-2024)



Source: Author's calculations are based on the National Cybersecurity Strategies (NCS) data (v1.0), collected by one of the authors.

Azmi, Tibben and Win (2016, 2) define a *national cybersecurity strategy* as "a careful plan or method of protecting both informational and non-informational assets through the ICT

infrastructure to achieve specific national goals over an extended period." The adoption of such a strategy represents a comprehensive national effort to tackle the challenges and leverage the opportunities presented by the Internet, signaling the growing importance that a country's leadership places on cybersecurity both domestically and internationally. These strategies typically include high-level objectives, principles, and priorities guiding the country's approach to cybersecurity, detail the planned actions to achieve these goals, and assign responsibilities to relevant stakeholders—establishing the cybersecurity agenda and apparatus for the foreseeable future (International Telecommunications Union, 2010, 13).

Studying the global diffusion of inaugural national cybersecurity strategies is essential in today's digitally interconnected world. These strategies represent a country's earliest mechanism for managing cyber threats and reflect how states start prioritizing technological risk amid rising digital dependence. Their adoption not only shapes domestic institutions and policies but also contributes to international cooperation, norm-setting, and the broader governance of cyberspace. Analyzing when and why countries adopt these strategies sheds light on how governments respond to evolving cross-border threats, reveals the influence of international organizations and other key actors, and uncovers the mechanisms through which policy ideas spread. Importantly, examining cybersecurity policy diffusion offers valuable insights into broader patterns of policy adoption and the conditions that facilitate or hinder uptake across countries and regions.

Policy adoption is a critical area of study across a range of issues (Berry and Berry, 1990; Rogers, 1995; Simmons and Elkins, 2004; Brooks, 2005; Fordham and Asal, 2007; Simmons, Lloyd and Stewart, 2018). Despite the Internet's profound societal impact, the adoption of cybersecurity policy remains relatively understudied. Existing research often focuses on individual countries (Bartlett, 2018; Huang and Li, 2018), or specific regions

(Dunn-Cavelty, 2005), and tends to be primarily descriptive, rather than explanatory. These studies suggest that threats (Azmi, Tibben and Win, 2016; Dunn-Cavelty, 2005; Luiijf, Besseling and De Graaf, 2013) or engagement with international organizations (Azmi, Tibben and Win, 2016; Heiding, O'Neill and Price, 2025) may be key drivers. However, there is no clear consensus on what drives the global diffusion of national cybersecurity strategies.

Addressing this gap requires comprehensive, systematic data that enables cross-national comparison and theory testing. To that end, we introduce a new panel dataset covering national cybersecurity strategies in 193 countries from 2000 to 2024. While existing repositories—such as those maintained by the International Telecommunication Union, the NATO Cooperative Cyber Defence Centre of Excellence, and the United Nations Institute for Disarmament Research—offer valuable collections, they often fail to distinguish between substantively different types of cybersecurity initiatives, potentially overstating strategy adoption. Our National Cybersecurity Strategies (NCS) data (v1.0) addresses this limitation by meticulously selecting pertinent documents from official government websites and engages, as needed, with country experts to ensure their accuracy and relevance. This dataset, therefore, offers a reliable empirical foundation for scholars seeking to explore cross-national patterns, evaluate theoretical claims, and generate new insights regarding the drivers and consequences of policymaking in global and comparative contexts.

Leveraging this new dataset, we apply a survival model to analyze the timing of countries' inaugural national cybersecurity strategies. To assess which mechanisms most consistently account for the global spread of these strategies, we draw on two leading explanations for cybersecurity-policy diffusion—the cyber-threat environment and membership in international organizations—as well as an additional mechanism: international

military alliances. While military alliances have been a prominent explanation for policy diffusion more broadly, they have not previously been applied to cybersecurity policy specifically. Our analysis, which covers all 193 countries from 2000 to 2020, finds robust empirical evidence that all three mechanisms contribute to diffusion, with international-organization membership having the strongest effect.

This finding helps explain the notable surge in the adoption of national cybersecurity strategies after 2010. During the 2000–2009 period, only ten countries had adopted such strategies, compared to 109 between 2010 and 2020. This growth meant that alliances began to play a more prominent role only in the post-2010 period, as the increasing number of allied countries with strategies made policy emulation more feasible. The post-2010 period also coincides with a marked rise in the frequency and visibility of major cyber-attacks—such as the discovery of Stuxnet in 2010, North Korea's attack on Sony in 2014, Russian operations targeting Ukrainian power infrastructure in 2015 and 2016, among others. In parallel, intergovernmental organizations increasingly began addressing cybersecurity: of the 137 IGOs that engaged with the issue during the study period, 101 did so after 2009.

Our study offers two significant contributions. Firstly, our cross-national approach provides a systematic understanding of the global diffusion of national cybersecurity policies. By assessing the impact of competing or complementary explanations, our findings enrich both academic and policy discussions on the drivers of national cybersecurity strategies and contribute to broader debates on international security collaborations, technological innovation impacts, and geopolitical influences.

Secondly, by introducing a new dataset of national cybersecurity strategies, our study offers a valuable resource for scholars of international relations and global governance. Beyond enabling the study of cybersecurity policy itself, the dataset facilitates inquiry

into broader IR questions—such as the effectiveness of national strategies, regional patterns of governance, and the alignment between state rhetoric and policy implementation. It also opens the door to comparative analysis across policy domains. When used alongside datasets on national approaches to emerging technologies, trade, or environmental policy, researchers can examine how states respond to complex transnational challenges, how policy ideas diffuse across borders, and how global norms take shape in the digital age.

Drivers of Global Cybersecurity-Strategy Diffusion

Scholars have long been intrigued by why and when actors adopt certain policies (Walker, 1969; Berry and Berry, 1990; Shipan and Volden, 2008; Simmons and Elkins, 2004; Simmons, Lloyd and Stewart, 2018). Building on this foundation, existing literature identifies two principal explanations for the global diffusion of national cybersecurity strategies: the influence of the cyber-threat environment (Azmi, Tibben and Win, 2016; Dunn-Cavelty, 2005; Luiijf, Besseling and De Graaf, 2013) or membership in international organizations (Azmi, Tibben and Win, 2016; Heiding, O'Neill and Price, 2025). We complement these explanations with an additional one—the dynamics of alliances—which has been shown to drive diffusion in other policy areas (Long, Nordstrom and Baek, 2007; True and Mintrom, 2001) and also to explain diffusion of military cyber capabilities (Kostyuk, 2024, 2025). Below, we briefly discuss each of these drivers.

Explanation #1: Cyber-Threat Environment

Prior studies have explored the role of threats in driving policy adoption across various issues, including climate change, criminal law, environment, and energy (Steves and Teytelboym, 2013; Stern, Dietz and Vandenbergh, 2022). Cybersecurity policy is no ex-

ception. For instance, Gomez (2016) demonstrates that states are inclined to revise their cybersecurity policies in response to cyber risks. Additionally, Valeriano and Maness (2015) discuss how the cyber-threat environment serves as a tool for politicians to advocate policy changes.

A descriptive analysis of approximately sixty documents outlining strategies adopted by fifty-four countries reveals a common concern with national vulnerability to cyber threats, with forty-six of these documents explicitly referencing such risks (Azmi, Tibben and Win, 2016). This concern is clearly reflected in the 2009 UK national cybersecurity strategy, in which section titled "Why does the UK need a Cyber Security Strategy?" highlights the country's "greater exposure to the rapidly evolving threats and risks" and emphasizes that "a strategic approach is fundamental" to the government's ability to lead a coherent national response to these challenges (UK Cabinet Office, 2009, 9). Similarly, the 2017 Israeli national cybersecurity strategy mentions that its purpose is, "first and foremost, a means of realizing the Israeli cyber vision by keeping cyberspace safe and by confronting various cyber threats" (Israel's National Cyber Directorate, 2017, 5).

Importantly, several high-profile cyber incidents appear to have contributed to surges in cybersecurity strategy adoption or revision across countries. Events such as Titan Rain (a series of cyber-espionage attacks in the early 2000s), Stuxnet (a sophisticated cyber-weapon discovered in 2010), and NotPetya (a destructive malware attack in 2017) highlighted the real-world consequences of cyber threats and served as wake-up calls for governments. These incidents not only demonstrated the growing sophistication of state and non-state cyber actors but also revealed the global reach and spillover effects of cyber operations, increasing the sense of urgency among policymakers worldwide.

These examples suggest that countries adopt cybersecurity strategies not only in response to specific cyber incidents but also based on their perceptions of a shifting, often

regionalized, threat environment. For instance, Qatar's 2014 national cybersecurity strategy explicitly notes not only that the country was among those "most affected by targeted attacks in 2013" but that its geographical region (the Middle East and North Africa) was among the most targeted at around the same time (Ministry of Information and Communications Technology, 2014, 4). Similarly, Chile's 2017 national cybersecurity strategy expresses concern about the regional cyber landscape, noting that "regionally, the countries that have reported the highest number of cyber attacks in Latin America were Brazil, Argentina, Colombia, Mexico and Chile" (Government of Chile, 2017, 36).

Not all strategies, however, are triggered by clearly identified incidents. The 2009 UK strategy, for instance, does not cite any specific cyber-attacks, but instead highlights the nation's increasing dependence on digital infrastructure as a source of growing risk (UK Cabinet Office, 2009). This absence of attribution does not necessarily imply a lack of threats; rather, it may reflect strategic, political, or diplomatic choices to remain neutral, avoid assigning blame, or downplay vulnerabilities. Whether countries act in response to concrete events or more diffuse threat perceptions, the experience—or anticipation—of cyber risk plays a central role in shaping strategic responses. One of the most common responses seems to be the adoption of a national cybersecurity strategy.

These strategies offer comprehensive, coordinated frameworks to protect a country's digital assets from evolving cyber-threats. By setting clear objectives and policies, a cybersecurity strategy promotes a unified approach across government agencies, the private sector, and international partners. Moreover, it guides investments in cybersecurity awareness, technological innovation, and digital infrastructure defense. Ideally, this proactive posture not only reduces vulnerabilities but also enhances national security, fosters economic stability, and strengthens public trust in digital systems in an increasingly interconnected world.

Hypothesis 1 (Cyber-Threat Environment): *Countries are more likely to adopt their first national cybersecurity strategies in response to perceived increases in cyber threats.*

Explanation #2: Cyber-Relevant International-Organization Membership

Prior research shows that the exchange of information among connected actors is a driving force behind diffusion of many sociological processes (Rogers, 1995). For example, international organizations facilitate the diffusion of various innovations at a lower cost because membership in such organizations can allow states to quickly acquire necessary knowledge and expertise from other members who have already adopted a particular innovation.

Prior research has shown that membership in international organizations can facilitate the development of a country's first national cybersecurity strategy (Azmi, Tibben and Win, 2016; Heiding, O'Neill and Price, 2025). By cooperating through IGOs, states benefit from economies of scale in accessing cybersecurity expertise, frameworks, and resources. Multilateral institutions such as the ITU and NATO have issued guidelines to help member states design national strategies aligned with international standards (Heiding, O'Neill and Price, 2025). This shared approach can standardize best practices, create a common language for cybersecurity policy, and improve coordination among nations—while also reducing the cost and complexity of developing strategies independently.

The Organization of American States (OAS) offers a vivid example of how intra-organizational cybersecurity-information exchange can increase the likelihood that members adopt their first national cybersecurity strategy. In 2004, the OAS developed a regional cybersecurity strategy that constituted a multidimensional approach to creating a culture of cybersecurity. In addition, the OAS Inter-American Committee Against Ter-

rorism (CICTE) created a specific cybersecurity program for the region meant to help states develop and implement their first national cybersecurity strategies (Organization of American States, 2024). The regional strategy serves as a rulebook, and the cybersecurity program provides access to resources that allow countries to adopt national cybersecurity strategies that follow this rulebook.

In addition, the OAS has been visiting its member states—including Colombia, Panama, and Trinidad and Tobago—to provide them with direct assistance in developing their national cybersecurity strategies. In 2014, for instance, the OAS collaborated with the government of Jamaica to conduct a two-day event in Kingston during which it helped the country draft its first national cybersecurity strategy. The OAS also brings country experts together with the goal of helping them acquire new knowledge that they can then use to develop national cybersecurity strategies back home. In 2017, Canada signed a multi-million dollar project of this kind with the OAS to enhance the cybersecurity skills of many national entities (Organization of American States, 2017). As of 2020, this OAS involvement has led eighteen countries from Latin America and the Caribbean to make significant strides towards establishing their first national cybersecurity strategies (Bianchi, 2022).

For these reasons, we hypothesize that the more cyber-relevant IGOs a country is a member of—even if cybersecurity is not the organization's primary focus—the more likely it is to adopt its inaugural national cybersecurity strategy.

> ***Hypothesis 2 (Cyber-Relevant International-Organization Membership):*** *Countries that are members of cyber-relevant international organizations (i.e., those that address cybersecurity issues to some extent, even if not as a primary focus) are more likely to adopt their first national cybersecurity strategy.*

Explanation #3: Influence of Allies

Not all organizations are likely to have an equal impact on the cybersecurity-adoption process. The above example shows that international alliances can be particularly relevant, given nations' desire to address transnational cybersecurity threats collectively. Prior literature points to the important role allies play in certain policy areas, such as environmental, technological, and social policy, by sharing necessary knowledge required for policy adoption (Long, Nordstrom and Baek, 2007; True and Mintrom, 2001).

Alliances also play a significant role in shaping national cybersecurity efforts (Kostyuk, 2024). For instance, Kostyuk (2024) shows that allies with advanced military cyber capabilities frequently support their less-equipped partners by sharing technical expertise, offering training programs, and providing tailored capacity-building initiatives. These efforts are often designed to address specific institutional or technical gaps in the partner country, ultimately helping them establish more resilient cyber-defense infrastructures. Alliances also facilitate workshops, joint exercises, and the exchange of best practices that contribute to the development of national cybersecurity frameworks (King, 2014; UNIDIR, 2024).

Given that the adoption of a first national cybersecurity strategy typically marks a country's initial public commitment to addressing cyber threats through coordinated national policy, the influence of allies—particularly those with established strategies—can be especially significant. Allies with prior experience often provide not only technical resources and institutional support, but also policy models and political legitimacy that can encourage or accelerate strategy adoption. These relationships can operate through direct assistance, such as training and capacity building, or through broader alliance-based diffusion, where norms and expectations around cybersecurity policymaking spread among partners. A clear example of this dynamic appears in Romania's 2013 national cybersecurity strategy, which explicitly cites the national strategies of its NATO allies—Estonia, the

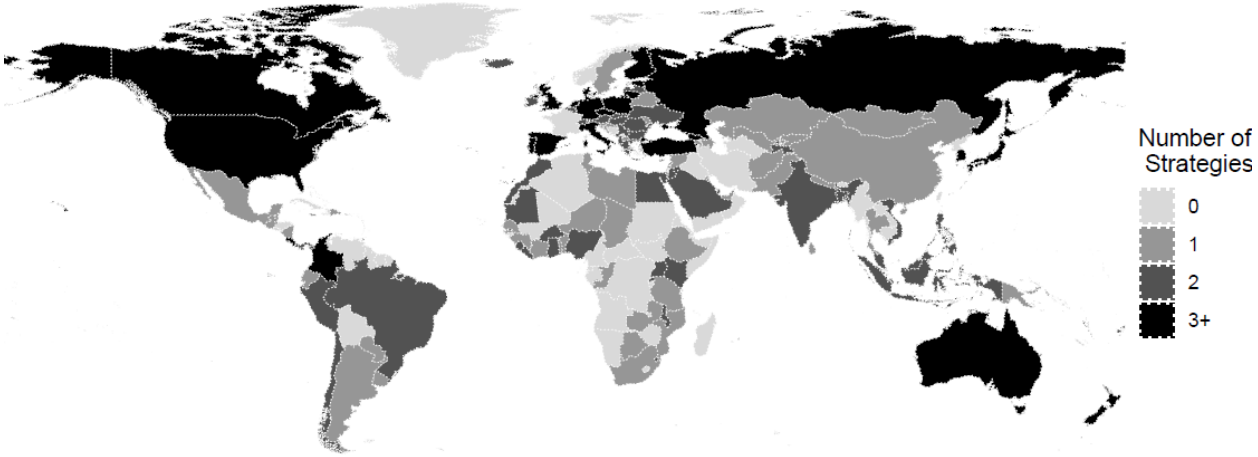
United States, the United Kingdom, Germany, and France—as setting "the framework for action and cooperation" and serving as examples for Romania to follow (Government of Romania, 2013, 1). This illustrates how alliance networks not only facilitate the transfer of knowledge and capabilities but also legitimize and shape the timing of strategic policy adoption.

> ***Hypothesis 3 (Influence of Allies):*** *Countries are more likely to adopt their first national cybersecurity strategies when their allies have already adopted such strategies.*

New Data on National Cybersecurity Strategies

We have compiled a comprehensive dataset of national cybersecurity strategies, titled the National Cybersecurity Strategies (NCS) dataset (v1.0). This dataset includes 246 strategies adopted by the 193 UN-recognized states between 2000 and 2024. Over this 24-year period, some countries released multiple strategies, while others have published only their first. Overall, our dataset records 246 strategies adopted by 135 countries.

Figure 2: TOTAL NUMBER OF NATIONAL CYBERSECURITY STRATEGIES PER COUNTRY (2000-2024)



Source: Author's calculations are based on the National Cybersecurity Strategies (NCS) data (v1.0), collected by one of the authors.

Figure 2 presents the total number of strategies adopted by each country during the study period. Japan stands out with the highest number of strategies (seven). In contrast, many countries, such as Armenia and Belize, have adopted only a first strategy. A few countries, including Bhutan and Bolivia, have yet to publish one at all. For these countries, our dataset records the absence accordingly.

To ensure the relevance and reliability of the data, we primarily sourced the strategy documents from official government websites. In line with best practices in conflict studies, we cross-referenced multiple sources to validate the inclusion and content of each strategy (Woolley, 2000). Specifically, we consulted databases curated by international organizations such as the ITU, NATO CCDCOE, and UNIDIR. Given the linguistic diversity of the documents, we took several steps to address potential language barriers. Many strategies were published in English or in both English and the native language (e.g., Greece's 2018 strategy), and a significant number were written in widely spoken languages such as Russian, Spanish, and French—languages in which our research team has fluency. In cases where documents were only available in other languages, multilingual team members reviewed the texts to ensure accurate interpretation. Where information remained limited or ambiguous, we attempted to contact country-specific experts and, when possible, government officials. Although responses were not always forthcoming, we are confident that these practices enabled us to compile the most accurate and comprehensive dataset currently available.

The NCS dataset has two main components:

1. **Structured Metadata Spreadsheet:** This Excel file records key information for each strategy, including the publication date, official title, governmental body responsible for its release, strategy length, and language of publication (e.g., English, native language, or both). While strategies may be authored by different national enti-

ties (e.g., the White House in the U.S., the Ministry of Science, Technology And Innovation in Japan), we have ensured that the dataset includes only national-level cybersecurity strategies—those that outline a country's overarching cyber policy.[1]

2. **Full-Text Repository:** The dataset also includes the original strategy documents in PDF format, provided in the language(s) in which they are published. We also converted the PDFs to plain text (.txt) files. We used Marker AI (version 0.1), an AI-based PDF processing tool, to process the PDF files. Each processed PDF was output as a dedicated folder. Every Marker folder contains a Markdown file and a text (.txt) file with the extracted text, along with image files corresponding to illustrations extracted from the original PDFs. A few PDFs could not be processed using Marker AI due to certain PDFs not including an explicit text layer. For these cases, the text files (referred to as Non-Marker files) were created using an Optical Character Recognition (OCR) technique.[2] This alternative method extracted only the text, and no illustrations were retrieved.[3] These text files enable various forms of computational analysis—such as content comparison, thematic mapping, topic modeling, and tracking of the evolution of policy language over time and across regions.

The full dataset, including the spreadsheet and all associated documents, are available on the National Cybersecurity Strategy website: https://sites.google.com/view/nationalcyberstrategies/home. We plan to update the dataset on a regular basis (e.g., every other year) to incorporate newly published strategies and any revisions to existing ones.

[1] Future versions of this dataset will include agency-specific strategies (e.g., a Ministry of Transportation's cybersecurity policy), international cybersecurity strategies, and other broader digital policy documents (e.g., digital agendas, e-government strategies, etc.).

[2] For more information on the OCR technique, see see.

[3] There were also a few strategies where we were not able to find pdfs (see Online Appendix Section 1).

Data & Empirical Strategy

Dependent Variable. Our dependent variable is the adoption of a country's first general, government-wide national cybersecurity strategy (`Adoption`) during the 2000–2020 period.[4] Countries are coded as "1" if they enacted such a strategy during this time, and "0" if they did not. This variable is constructed using the NCS dataset (v1.0), introduced above. Of the 161 countries included in the analysis, 119 adopted their first national cybersecurity strategy during the observed period.[5]

Figure 3 shows the global spread of cybersecurity strategies over four five-year intervals.[6] It reveals notable variation in the timing of adoption, with clear patterns of early leaders and latecomers. For example, countries such as Russia, the United States, Canada, and many in Western Europe began developing national strategies as early as the early 2000s. In contrast, countries in Eastern Europe, Central Asia, and Latin America—including Mexico—introduced their first strategies much later.

Main Predictors. Here we explain how we measure each of the three potential explanations of cybersecurity-strategy diffusion. First are external cyber-threats, both actual and perceived. We measure actual threats by the number of large, known cybercampaigns[7] that a country experienced in the year preceding its strategy adoption (`Country-Specific Cyber-Attacks`).[8] To create this variable, we use Valeriano, Jensen and Maness 2018's Dyadic Cyber Incident Dataset (DCID) (2.0)—one of the few available datasets on major,

[4] We focus our analysis on this period as some of our covariates are available only during this period.

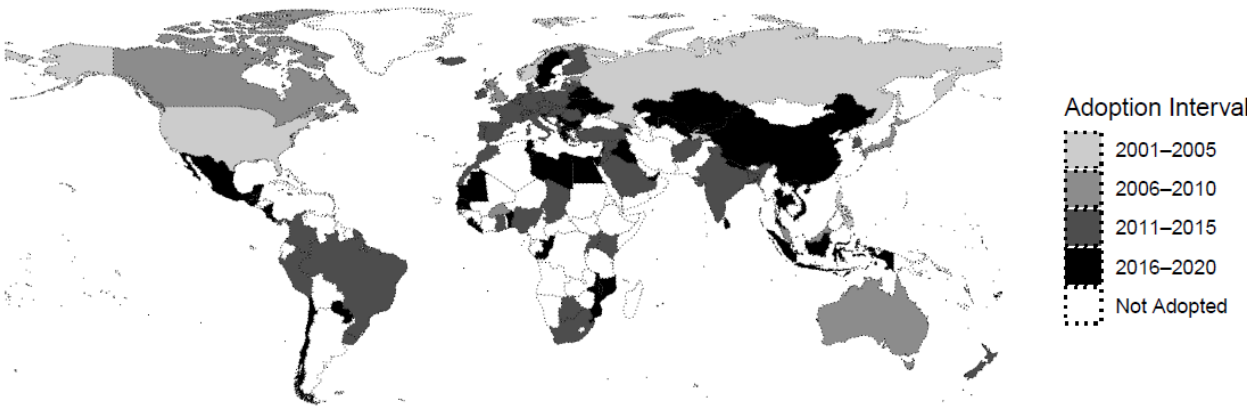
[5] Due to missing data for some covariates, a number of countries were excluded from the final sample.

[6] Russia, which adopted its first strategy in 2000, included in the 2001-2005 period.

[7] Valeriano, Jensen and Maness (2018) define a cybercampaign as an accumulation of cyber-attacks meant to achieve strategically important goals.

[8] Since a Cox Proportional-Hazards model—a model that we use in our analysis, details of which we explain below—captures any changes in a global cyber-threat environment over time, we do not include any additional variables to capture this change.

Figure 3: COUNTRIES GROUPED BY YEAR OF STRATEGY ADOPTION OVER 5-YEAR INTERVALS (2000-2020)



Source: National Cybersecurity Strategies (NCS) data (v1.0) collected by one of the authors. Russia, which adopted its first strategy in 2000, included in the 2001-2005 period.

known cyber campaigns. In addition to using DCID, we also use the European Repository of Cyber Incidents (v1.0) as a source of cyber-threats (EuRepoC, 2022).

To further assess the impact of cyber threats, we include a measure of the annual number of cyber-attacks that occurred in the previous year within a country's region (`Regional Cyber-Attacks`) to capture perceived cyber threat levels. Regional classifications are based on the World Bank's definitions of world regions.

Our second explanation focuses on the influence of international organizations. As outlined in our theory, we measure this influence by counting the number of IGOs that a country is a member of that engage with cybersecurity issues in a given year (`Cyber-Relevant IGO Memberships`). Using the dataset from Pevehouse et al. (2019), we track the year in which each IGO began addressing cybersecurity topics. Out of more than 500 IGOs in the dataset, 137 began engaging with cybersecurity in various capacities during the study period. For a complete list of IGOs, see Online Appendix Section 4.

Lastly, to assess the influence of alliances, we calculate a weighted average effect of the cybersecurity strategies adopted by a country's defensive allies prior to the adoption of its own first national strategy (`Strategies Adopted by Allies`). To identify defensive

allies, we rely on Leeds et al. (2002)'s Alliance Treaty Obligations and Provisions (ATOP) dataset (v5.0), which offers a detailed and comprehensive account of alliance relationships over the studied period. We then use the NCS dataset (v1.0) to determine which of these allies had already adopted national cybersecurity strategies at the time a given country adopted its own. We apply lagged network-weighted effects to represent the average influence of allies, assigning weights based on their relative importance to the country in question.[9]

Additional Controls. We account for the following variables in our analysis. First is the country's wealth measured by its GDP per capita taken from the World Bank (`GDP per Capita`).[10] Second is the country's level of technology measured by the number of Internet users as a percentage of the country's total population, taken from the World Bank (`Internet Users per Capita`).[11] Third, since democracies are known to be more transparent in their policies and are more likely to provide the public good of security, we account for a country's regime type. Using Gurr, Marshall and Jaggers (2010)'s Polity IV score, we create a dummy variable that takes the value of 0 if this score is less than six, which represents an autocracy, and the value of 1 if this score is at least six, which represents a democracy (`Democracy`). Using the World Bank data, we also control for regions, as they differ in their exposure to cyber attacks. Africa is the baseline category.

Method. We use an event history model[12] that focuses on the spell of time until the adoption of a national cybersecurity strategy occurs. Specifically, we employ the Cox

[9] Additional details on the calculation of the weighted-average effects are provided in Online Appendix Section 3.1.

[10] We use a logarithmic transformation to address this variable's skewness.

[11] We use a logarithmic transformation to address this variable's skewness. Since `GDP per Capita` and `Internet Users per Capita` are highly correlated (82%), we include only `Internet Users per Capita` into our analysis. But we run models with both variables as our robustness checks.

[12] Event history models have become a common tool for studying policy diffusion (Berry and Berry, 1990; Simmons and Elkins, 2004; Simmons, Lloyd and Stewart, 2018).

Proportional-Hazards (CPH) model which tests for conditions that create a greater risk of the country adopting its first cybersecurity strategy.[13] Our unit of analysis is the country-year. The analysis begins in 2000, one year before Russia adopted its first national cybersecurity strategy and around the time most cyber-threat datasets began tracking incidents. The analysis ends in 2020. If the country in question has not adopted a cybersecurity strategy by December 31, 2020, it is right-censored in our data set. Lastly, since many of the covariates change over time, we use interval censoring to capture time-varying covariates (Therneau and Grambsch, 2000).

Findings

Our main finding is that all three factors—actual (as opposed to merely perceived) cyber threats, membership in cyber-relevant international organizations, and military alliances with countries that have adopted cybersecurity strategies—contribute to the global diffusion of inaugural national cybersecurity strategies, with international-organization membership having the strongest effect. Tables 1 and 2, which present the results, show positive statistically significant associations between `Country-Specific Cyber-Attacks` and `Adoption`, between `Cyber-Relevant IGO Memberships` and `Adoption`, as well as between `Strategies Adopted by Allies` and `Adoption`, with hazard ratios consistently larger than one.[14] Below, we review these findings in detail.

We begin by examining the cyber-threat environment as a potential driver of cybersecurity strategy diffusion. Models 1 and 2 focus on actual cyberattacks a country has experienced. Model 1, using DCID data, shows a positive and statistically significant re-

[13] Online Appendix Section 3.2 provides a detailed explanation of the Cox Proportional-Hazards model and its assumptions and various diagnostic tests. We also use a discrete time-series model as our robustness check (Online Appendix Section 5.3).

[14] We use hazard ratios to present our results. Hazard ratios larger than one identify positive correlation and those smaller than one identify negative correlation.

Table 1: EXPLAINING THE GLOBAL DIFFUSION OF NATIONAL CYBERSECURITY STRATEGIES (HAZARD RATIOS AND CONFIDENCE INTERVALS)

	Threats			
	Model 1	*Model 2*	*Model 3*	*Model 4*
Country-specific cyber-attacks (lag,sc) (DCID)	1.1**(1.03; 1.16)	——	——	——
Country-specific cyber-attacks (lag,sc) (ERC)	——	1.52**(1.14; 2.03)	——	——
Regional Cyber-attacks (lag,sc) (DCID)	——	——	0.63^(0.39; 1.02)	——
Regional Cyber-attacks (lag,sc) (ERC)	——	——	——	1.32(0.81; 2.17)
Democracy	2.05**(1.31; 3.21)	2.06**(1.27; 3.34)	2.07**(1.31; 3.27)	2.06**(1.3; 3.27)
Internet Users (log,sc)	3.16***(1.88; 5.28)	2.67***(1.59; 4.47)	3.24***(1.94; 5.43)	3.18***(1.91; 5.28)
Asia	0.98(0.5; 1.9)	0.57(0.26; 1.25)	3.99^(0.85; 18.86)	0.76(0.29; 1.96)
Europe	1.05(0.52; 2.14)	0.83(0.4; 1.76)	1.56(0.66; 3.69)	0.82(0.36; 1.88)
North America	0.69(0.31; 1.51)	0.88(0.41; 1.89)	1.81(0.49; 6.7)	0.86(0.36; 2.05)
Oceania	1.7(0.6; 4.81)	2.03(0.72; 5.74)	1.94(0.62; 6.06)	2.18(0.8; 6)
South America	0.39^(0.15; 1.01)	0.5(0.2; 1.27)	0.39^(0.15; 1.02)	0.56(0.19; 1.61)
Concordance	0.75	0.76	0.75	0.74

Note: This table examines the threat-related drivers behind the global diffusion of national cybersecurity strategies. The results, based on a Cox Proportional-Hazards model, indicate that only threats directly targeting countries contribute to this diffusion. There are 2,649 observations and 107 events. All results are based on two-tailed tests. Models with `Internet Users per Capita` do not include `GDP per Capita` because the two variables are highly correlated. `log`: logarithmized; `sc`: standardized; `lag`: lagged. ^p<0.1; *p<0.05; **p<0.01; ***p<0.001

Table 2: EXPLAINING THE GLOBAL DIFFUSION OF NATIONAL CYBERSECURITY STRATEGIES (HAZARD RATIOS AND CONFIDENCE INTERVALS) (CONTINUED)

	IO Membership	**Influence of Allies**	**All explanations**
	Model 5	*Model 6*	*Model 7*
Cyber-Relevant IGO Memberships (lag, sc)	14.55*(1.18; 180.06)	——	14.97*(1.19; 188.52)
Strategies adopted by allies (lag, sc)	——	1.14*(1.03; 1.26)	1.08*(1.01; 1.15)
Country-specific cyber-attacks (lag, sc) (DCID)	——	——	1.05*(1; 1.11)
Democracy	2.13**(1.34; 3.36)	2.17**(1.36; 3.46)	2.13**(1.35; 3.37)
Internet Users (log)	3.12***(1.86; 5.23)	3.1***(1.86; 5.18)	3.05***(1.82; 5.11)
Asia	1.12(0.58; 2.15)	1.12(0.59; 2.15)	1.1(0.56; 2.13)
Europe	1.07(0.52; 2.21)	0.93(0.46; 1.87)	1.02(0.5; 2.07)
North America	0.68(0.31; 1.49)	0.65(0.3; 1.42)	0.67(0.31; 1.48)
Oceania	1.71(0.6; 4.89)	1.68(0.61; 4.6)	1.72(0.61; 4.85)
South America	0.39^(0.15; 1.01)	0.37*(0.15; 0.96)	0.39*(0.15; 1)
Concordance	0.75	0.75	0.75

Note: This table focuses on the drivers of the global diffusion of national cybersecurity strategies, focusing on the effect of cyber-relevant IO membership, allies, and actual threats. The results show that all three factors are likely to contribute to this diffusion. Results are from a Cox Proportional-Hazards model. There are 2,649 observations and 107 events. All results are based on two-tailed tests. Models with `Internet Users per Capita` do not include `GDP per Capita` because the two variables are highly correlated. `log`: logarithmized; `sc`: standardized; `lag`: lagged. ^p<0.1; *p<0.05; **p<0.01; ***p<0.001

lationship between cyberattacks in the year prior to adoption and the likelihood of strategy adoption in the following year (HR: 1.10; CI: 1.03–1.16). Model 2, based on EuRepoC data, similarly shows a positive and statistically significant effect (HR: 1.52; CI: 1.14–2.03).

Models 3 and 4 shift focus to regional cyberattacks as a proxy for perceived threats. Model 3 (DCID regional data) finds a marginally statistically significant but negative association (HR: 0.63; CI: 0.39–1.02), while Model 4 (EuRepoC regional data) finds a non-significant, positive relationship (HR: 1.32; CI: 0.81–2.17). These findings offer partial support for *H1*.

We next examine the influence of cyber-relevant international organizations on the global diffusion of cybersecurity strategies. Model 5 was estimated using ridge regression due to near-perfect separation between `Cyber-Relevant IGO Memberships` and the outcome variable. Ridge regression helps address this issue by shrinking overly strong predictor effects, which can otherwise lead to unstable or inflated estimates. Even after applying this more conservative approach, the model shows a positive and statistically significant relationship between `Cyber-Relevant IGO Memberships` and `Adoption` (HR: 14.55; CI: 1.18–180.06).[15] This suggests that membership in cyber-relevant IGOs likely contributes to the spread of national cybersecurity strategies.

Model 6 examines a third possible driver—military alliance with a country that has already adopted a cybersecurity strategy—and shows that this is also likely to contribute to the diffusion of such strategies. This is demonstrated in the positive and statistically significant correlation between `Strategies Adopted by Allies` and `Adoption` (HR: 1.14; CI: (1.03, 1.26)). Finally, Model 7 includes all predictors simultaneously and applies ridge regression to ensure that we can more accurately compare the relative strength of

[15]The large coefficient and wide confidence intervals are due to the strong correlation between `Cyber-Relevant IGO Memberships` and time—a predictable pattern, as IGOs have increasingly engaged with cyber issues over the years. As a robustness check, we re-estimate the model after partialing out the time trend. The results remain robust (see Online Appendix Section 5.5).

each predictor's association with `Adoption`. The results show positive and statistically significant relationships for `Country-Specific Cyber-Attacks` (HR: 1.05; CI: 1.00–1.11), `Cyber-Relevant IGO Memberships` (HR: 14.97; CI: 1.19–188.52), and `Strategies Adopted by Allies` (HR: 1.08; CI: 1.01–1.15). Together, these results—presented in Tables 1 and 2—support *H1*, *H2*, and *H3*. Notably, the effect size is largest for `Cyber-Relevant IGO Memberships`, suggesting that institutional embeddedness plays the most substantial role in the diffusion of inaugural cybersecurity strategies.

Robustness Checks. Our findings are also robust to: (1) accounting trends among different alliances (NATO membership); (2) an alternative cyber-threat-environment measurement (strategies adopted by adversaries); and (3) an alternative model specification (generalized linear models). Lastly, under-reporting—particularly in regions outside North America and Europe—can introduce bias into cyber incident-level data. To assess whether our findings are sensitive to potential under-reporting, we re-run our main model using only data from regions with higher reporting confidence—specifically OECD countries. Our results generally hold. For more details on these robustness checks, see Online Appendix Section 5.

Suggested Applications of the NCS Dataset

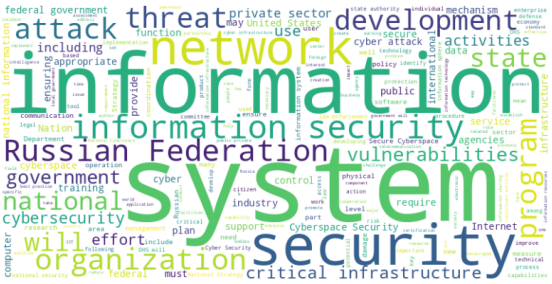
The previous section illustrates just one example of how the NCS dataset can be applied. More broadly, this dataset offers researchers a flexible and comprehensive resource for investigating a wide array of theoretical and empirical questions across cybersecurity, international relations, and comparative politics. Covering all 193 UN-recognized states from 2000 to 2024, the dataset provides rich, structured information on the timing, frequency, and content of national cybersecurity strategies. This structure enables both cross-sectional and longitudinal analyses, making it suitable for studying regional pat-

terns, temporal trends, and shifts in policy language over time.

To illustrate one such inquiry—namely, what national cybersecurity priorities look like and how they evolve—we generated word clouds from 97 inaugural national cybersecurity strategies published in English,[16] grouped into five-year intervals spanning 2000 to 2024. These visualizations highlight the most frequently used terms in each period, with word size reflecting relative frequency across strategies adopted during that timeframe. Figure 4 presents the resulting word clouds.

[16]See Online Appendix Section 6 for the list of strategies included in each period.

2000–2024



2000–2005

2006–2010

2011–2015

2016–2020

2021–2024

Figure 4: WORD CLOUDS BY PERIOD BASED ON NATIONAL CYBERSECURITY STRATEGY DOCUMENTS

One notable trend is the shifting prominence of the terms *cyber security* and *information security*. The former—commonly used by Western countries—typically reflects a narrower, more technical framing focused on confidentiality, integrity, and availability (the CIA triad). The latter—favored by countries like Russia and China—implies a broader scope, encompassing political and ideological concerns. The aggregated word cloud

(2000–2024) shows *cyber security* appearing slightly more frequently than *information security*. Zooming into individual periods, however, reveals that this was not always the case. The earliest period (2000–2005) is dominated by *information security*. From 2006–2010 onward, *cyber security* gains prominence—a trend that continues through subsequent periods (2011–2015, 2016–2020, 2021–2024). Future research could investigate whether this trend indicates a Western-led diffusion of terminology, or a deeper international convergence toward the *cyber security* framing—even among countries previously aligned with a more expansive *information security* paradigm.

Building on this exploration of terminology and framing, another relevant question is whether countries emulate one another in crafting their national cybersecurity strategies. To examine this, we analyze semantic embedding cosine similarity, which captures context, word order, and meaning by transforming documents into dense vector representations using a pre-trained language model.[17] Our focus is on inaugural strategies from members of the Five Eyes alliance and the Shanghai Cooperation Organization (SCO). Figure 5 shows the resulting similarity scores. Several strong pairings emerge, especially within the SCO: India–Pakistan (0.71), Belarus–Russia (0.69), and China–Pakistan (0.66). The Five Eyes countries also demonstrate notable alignment: Australia–New Zealand (0.71), USA–UK (0.65), and Canada–USA (0.61). These patterns suggest that geopolitical relationships may influence how countries semantically frame their cybersecurity strategies, though further analysis is needed to confirm causal links.

[17] We also computed Term Frequency–Inverse Document Frequency (TF-IDF) cosine similarity scores; see Online Appendix Section 6.

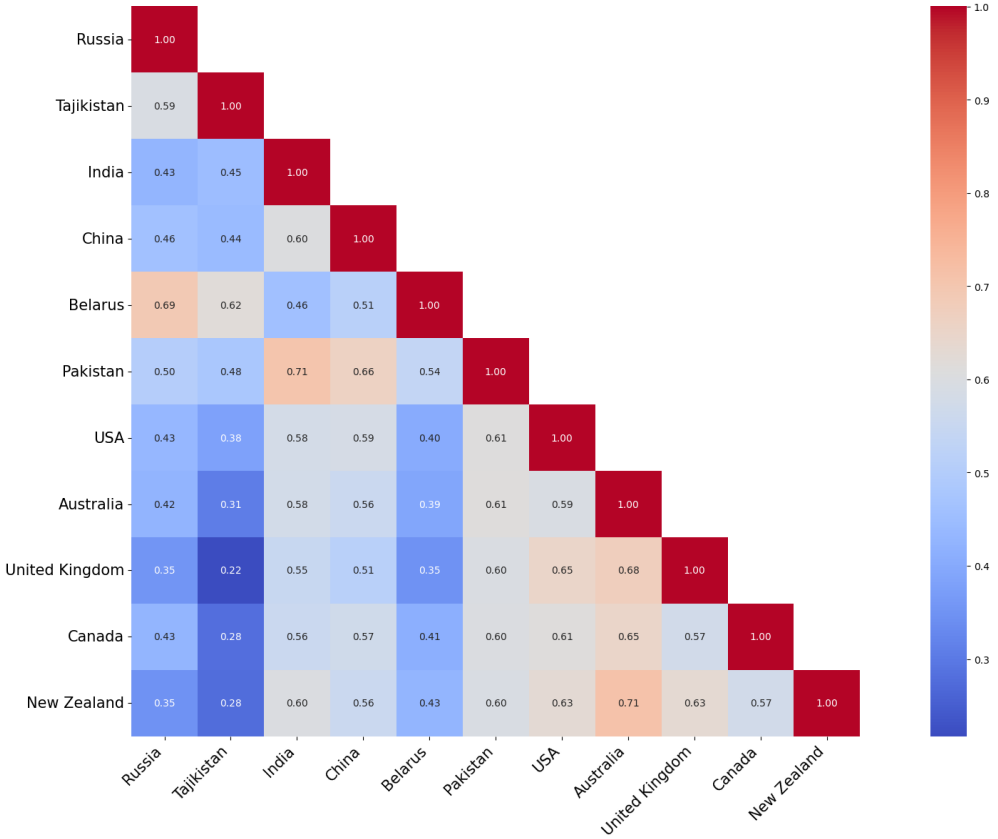


Figure 5: SEMANTIC EMBEDDING COSINE SIMILARITY OF INAUGURAL NATIONAL CYBERSECURITY STRATEGIES AMONG SELECTED COUNTRIES

Importantly, the NCS dataset can serve as either a dependent or independent variable, depending on the research question. As a dependent variable, it can help explain the conditions under which states adopt or revise cybersecurity strategies—for instance, in response to cyber incidents, technological diffusion, regional pressures, or shifts in regime type. As an independent variable, the dataset can be used to assess how the presence or content of national strategies shapes broader patterns of state behavior, such as participation in cyber norms-building initiatives, levels of international cooperation, or responses to cyber conflict.

Moreover, the dataset's flexibility allows it to be integrated with a range of complementary data sources—such as cyber conflict event datasets, economic indicators, alliance

networks, technological capacity indices, and regime classifications—to examine how cybersecurity policymaking interacts with broader issues of global governance, interstate competition, and digital security. Its compatibility with both qualitative case studies and large-scale quantitative research makes it a valuable tool for exploring how national strategies reflect and influence the rapidly evolving landscape of international politics.

Discussion

This article explores the global adoption of national cybersecurity strategies, seeking to understand why some countries implement such policies while others do not. Existing research—often descriptive rather than explanatory and focused on specific countries or regions—typically attributes adoption to rising cyber threats or the influence of international organizations (IOs). To test both established explanations (threats and IOs) and a novel one—diffusion after military alliances—we introduce the National Cybersecurity Strategies dataset, which systematically tracks when and how countries have adopted these strategies. We find that the strongest predictor of adoption is international-organization membership, highlighting the crucial role of international networks in shaping cybersecurity policy.

Our study contributes to the policy-diffusion literature by showing that international organizations play a central role in explaining the global spread of national cybersecurity strategies. While military alliances and the cyber-threat environment also contribute—each exerting a comparable but smaller influence—our findings underscore the particularly strong effect of institutional embeddedness in international organizations. This pattern highlights the preventive nature of these strategies, suggesting that states increasingly prioritize resilience through partnerships and shared norms over reactive responses to threats.

International networks of partners and allies also facilitate knowledge transfer, enabling countries to draw on existing frameworks and expertise when designing their first cybersecurity strategies. These findings align with and extend the work of Kostyuk (2024, 2025), who show that alliances shape the diffusion of military cyber capabilities. Similarly, we find that alliances play a meaningful, though more modest, role in guiding the development of national cybersecurity policy through shared strategic goals and policy learning.

This research also expands the political science literature by shifting the focus from great-power competition, which typically dominates cybersecurity discussions, to the strategic behavior of weaker states in addressing their cybersecurity vulnerabilities. While military cyber capabilities often receive the most attention, cybersecurity strategies—though softer in nature—are critical, as they mark the initiation of a country's cybersecurity apparatus.

Finally, our study contributes to broader debates in political science on policy diffusion in the information age. As technological change accelerates and global interdependence grows, states increasingly turn to international partners to navigate complex cybersecurity challenges. The collaborative role of these networks—through innovation, intelligence sharing, and joint responses—not only shapes cybersecurity strategies but may also influence the diffusion of other emerging technologies. Future research should explore whether these dynamics extend to additional policy domains, offering insights into how cooperation drives policy adoption in an increasingly digital world.

References

Azmi, Riza, William Tibben and Khin Than Win. 2016. "Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.".

Bartlett, Benjamin. 2018. "Government as facilitator: How Japan is building its cybersecurity market." *Journal of Cyber Policy* 3(3):327–343.

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.

Bianchi, Tiago. 2022. "Latin America and the Caribbean: cybersecurity strategy by country and status 2020.".
URL: *https://www.statista.com/statistics/1149424/cybersecurity-strategy-latin-america-caribbean-country/statisticContainer*

Brooks, Sarah M. 2005. "Interdependent and domestic foundations of policy change: The diffusion of pension privatization around the world." *International Studies Quarterly* 49(2):273–294.

Dunn-Cavelty, Myriam. 2005. "A Comparative Analysis of Cybersecurity Initiatives Worldwide.".

EuRepoC. 2022. "European Repository of Cyber Incidents, Version 1.0.".
URL: *https://doi.org/10.5281/zenodo.1234567*

Fordham, Benjamin O and Victor Asal. 2007. "Billiard balls or snowflakes? Major power prestige and the international diffusion of institutions and practices." *International Studies Quarterly* 51(1):31–52.

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

Government of Chile. 2017. "National Cybersecurity Policy 2017–2022.". Accessed: 2025-04-16.
URL: *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National*$_S$*trategies*$_R$*epository/Chile*$_N$*CSP%2*

Government of Romania. 2013. "Cyber Security Strategy of Romania.". Accessed: 2025-04-16.
URL: *https://www.cyberwiser.eu/sites/default/files/RO*$_N$*CSS*$_2$*013*$_e$*n.pdf*

Gurr, Ted R, Monty G Marshall and Keith Jaggers. 2010. "Polity IV Project: Political Regime Characteristics and Transitions, 1800-2009." *Center for International Development and Conflict Management at the University of Maryland College Park* .

Heiding, Fred, Alex O'Neill and Lachlan Price. 2025. Cybersecurity Strategy Scorecard. Technical report Belfer Center for Science and International Affairs, Harvard Kennedy School.

Huang, Hsini and Tien-Shen Li. 2018. "A centralised cybersecurity strategy for Taiwan."

Journal of Cyber Policy 3(3):344–362.

International Telecommunications Union. 2010. "Guide to Developing a National Cybersecurity Strategy.".

Israel's National Cyber Directorate. 2017. "Israel National Cyber Security Strategy: In Brief.". Accessed: 2025-04-16.
URL: *https://openresearch-repository.anu.edu.au/server/api/core/bitstreams/2d2bf3c7-c75b-40b6-bb23-5b07a168ef96/content*

King, Nelson. 2014. "ONLINE SECURITY STRATEGY.".
URL: *https://www.caribbeanlife.com/online-security-strategy/*

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

Kostyuk, Nadiya. 2025. "Beyond Threats: How Allies and Bureaucratic Competition Shape the Initial Development of Military Cyber Capabilities." *International Interactions* p. 00223433241226559.

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

Long, Andrew G, Timothy Nordstrom and Kyeonghi Baek. 2007. "Allying for peace: Treaty obligations and conflict between allies." *The Journal of Politics* 69(4):1103–1117.

Luiijf, Eric, Kim Besseling and Patrick De Graaf. 2013. "Nineteen national cyber security strategies." *International Journal of Critical Infrastructures 6* 9(1-2):3–31.

Ministry of Information and Communications Technology. 2014. "Qatar National Cyber Security Strategy.".

Organization of American States. 2017. "Canada Commits Can$2.5 Million to the OAS to Promote Cybersecurity Initiatives.". Accessed: 2025-04-16.
URL: *https://www.oas.org/en/media*$_c$*enter / photonews.asp?sCodigo* $= FNE - 21173$

Organization of American States, x. 2024. "Cybersecurity Program.".
URL: *https://www.oas.org/ext/en/security/prog-cyber*

Pevehouse, Jon CW, Timothy Nordstrom, Roseanne W McManus and Anne Spencer Jamison. 2019. "Tracking organizations in the world: The Correlates of War IGO Version 3.0 datasets." *Journal of Peace Research* p. 0022343319881175.

Rogers, Everett M. 1995. *The Diffusion of Innovations*. 3rd edition ed. New York: Free Press.

Shipan, Charles R and Craig Volden. 2008. "The mechanisms of policy diffusion." *American journal of political science* 52(4):840–857.

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.

Stern, Paul C, Thomas Dietz and Michael P Vandenbergh. 2022. "The science of mitigation: Closing the gap between potential and actual reduction of environmental threats." *Energy Research & Social Science* 91:102735.

Steves, Franklin and Alexander Teytelboym. 2013. "Political economy of climate change policy.".

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

True, Jacqui and Michael Mintrom. 2001. "Transnational networks and policy diffusion: The case of gender mainstreaming." *International studies quarterly* 45(1):27–57.

UK Cabinet Office. 2009. "Cyber Security Strategy of the United Kingdom.". Accessed: 2025-04-16.
URL: *https://assets.publishing.service.gov.uk/media/5a7c69fb40f0b62aff6c17fc/7642.pdf*

UNIDIR. 2024. "The Cyber Index: International Security Trends and Realities.".
URL: *https://unidir.org/files/publication/pdfs//cyber-index-2013-en-463.pdf*

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

Valeriano, Brandon and Ryan C Maness. 2015. *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA.

Walker, Jack L. 1969. "The diffusion of innovations among the American states." *American political science review* 63(3):880–899.

Woolley, John T. 2000. "Using media-based data in studies of politics." *American Journal of Political Science* pp. 156–173.