Role of International Organizations and Formal Alliances in the Global Diffusion of National Cybersecurity Strategies

Nadiya Kostyuk[*] and Jen Sidorova[†]

March 30, 2024

Abstract

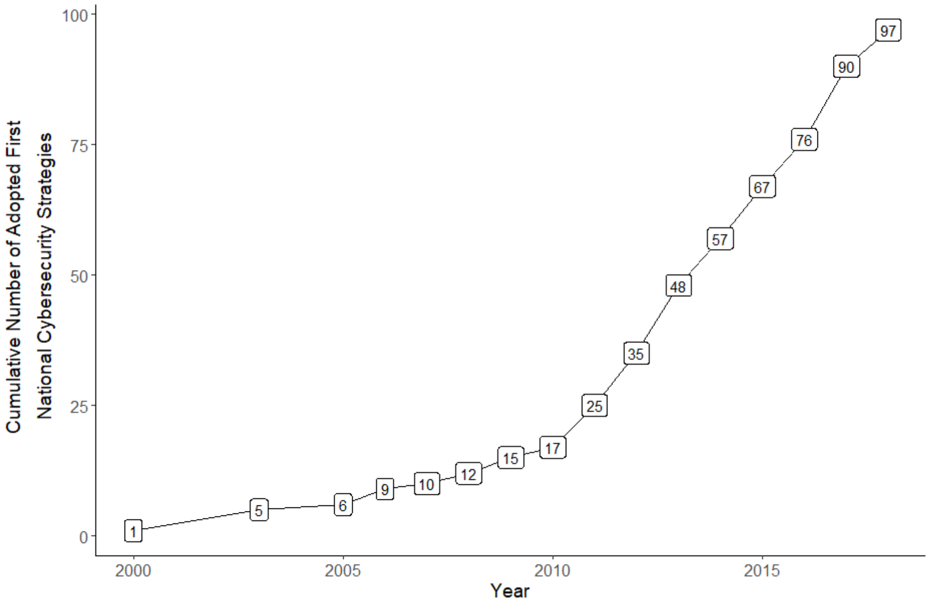
The politics of how countries design their national policies is a critical question in international relations because it has implications for domestic and international affairs. National cybersecurity strategies are the latest examples of policies that countries have been adopting, and they mark the significance of a country's leadership attributes to cybersecurity. Yet, there is limited theoretical and empirical work on the factors that explain this strategy diffusion. Using new data on national cybersecurity strategies between 2000 and 2018, this article shows that membership in international organizations and alliances are the most plausible drivers of this diffusion process. Our results are robust to a number of alternative specifications. The findings have important implications for the study of national security policy, innovation, and diffusion.

[*] Assistant Professor, School of Public Policy, Georgia Institute of Technology; nkostyuk3@gatech.edu

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

The politics of how nations design their national policies is a critical question in international relations because it has implications for domestic and international affairs. National cybersecurity strategies are the latest example of policies that countries have been adopting. The adoption of the first national cybersecurity strategy demonstrates to domestic and international communities the significance a country's leadership attributes to cybersecurity. These strategies outline high-level, nationwide objectives that a state plans to undertake to address opportunities and challenges presented by the Internet, carrying important implications for the global economy and security (Azmi, Tibben and Win, 2016).

Figure 1: *Adoption of the First National Cybersecurity Strategies (2000-2018)*



Source: Author's calculations are based on the National Cybersecurity Policies (NCSP) data (version 1.0), collected by the author.

Over the last decade, a large number of countries adopted their first national cybersecurity strategies. Figure 1 shows that by the end of 2010, seventeen countries adopted their first national cybersecurity strategy, seventeen countries adopted their first national cybersecurity strategy, whereas an additional eighty countries adopted their strategies over the next eight years. This begs the question: *What explains the post-2010 spike?* And more generally, *why and when do countries adopt their first national cybersecurity strategy?*

Studying why and when countries adopt their first national cybersecurity strategy is important for the following reasons. First, it allows us to better understand how governments respond to evolving threats posed by emerging technologies. Second, it sheds light on the role of actors and institutions in shaping global cybersecurity governance. Lastly, analyzing policy diffusion can provide insights into the broader dynamics of policy adoption across countries and regions.

Policy diffusion has been a subject of scholarship inquiry for decades (Berry and Berry, 1990*a*; Simmons and Elkins, 2004; Simmons, Lloyd and Stewart, 2018). Despite the centrality and importance of the Internet for global politics, we know surprisingly little about the factors that drive the adoption of national policies meant to address its impact on society. Most of the works are country- or region-specific (Azmi, Tibben and Win, 2016; Dunn-Cavelty, 2005; Johnsen, 2015; Lehto, 2013; Luiijf, Besseling and De Graaf, 2013; Min, Chai and Han, 2015; Sabillon, Cavaller and Cano, 2016; Sarker et al., 2019; Osho and Onoja, 2015; Cheung, 2018; Aggarwal and Reddie, 2018; Bartlett, 2018; Huang and Li, 2018; Abdullah, Mohamad and Yunos, 2018; Tambo and Adama, 2017; Catota, Morgan and Sicker, 2019).

To explain this puzzle, we build on works that explain policy diffusion. We supplement existing explanations identified in this literature with the anecdotal evidence collected from reviewing primary and secondary sources, including but not limited to national cybersecurity strategies, policy briefs, testimonies and speeches by the government officials. We have identified three potential diffusion drivers: threat environment, influence of international organizations, and influence of common culture and language. To test these potential theoretical explanations, we apply a survival model to newly collected data of official national cybersecurity strategies between 1999 and 2018. The analysis provides robust empirical support that international organizations—international alliances, in particular—are likely to explain the global diffusion of national cybersecurity strategies.

The paper proceeds as follows. We start to explain why studying the global diffusion of national cybersecurity strategies is important. We next present an overview of existing works on the policy diffusion topic. We then outline our three potential drivers of the adoption of the cybersecurity strategy. Next, we introduce a new dataset on national cybersecurity strategies and major explanatory variables that we will construct to run our analysis. We then present our empirical strategy and summarize the paper's empirical findings. Lastly, we offer a discussion of the broader significance of these results and provide concluding remarks.

Why Study Diffusion of Cybersecurity Strategies

Azmi, Tibben and Win (2016, 2) define *national cybersecurity strategy* as "a careful plan or method of protect[ing] both informational and non-informational assets through the ICT infrastructure for achieving...particular national goals usually over a long period of time." These strategies generally express "high-level objectives, principles and priorities that guide a country in addressing cybersecurity"; describe the steps that the country will undertake to achieve these objectives; list the stakeholders responsible for undertaking these steps; and set the country's cybersecurity agenda over the next few years (InternationalTelecommunicationsUnion, 2010, 13). The adoption of a national cybersecurity strategy marks the first nation-wide efforts to address challenges and opportunities presented by the Internet and communicates to domestic and international communities the rising significance a country's leadership attributes to cybersecurity.

Here are four main reasons to study the diffusion of national cybersecurity policies.

First, as cybersecurity threats continue to evolve and expand across borders, it is essential to understand how governments respond and adopt to these challenges. Examining the spread of cybersecurity policies can provide insights into the diffusion of best practices and innovative approaches, as well as the challenges and limitations faced by different countries. Second, understanding the factors that drive policy diffusion can shed light on the role of various actors and institutions, such as international organizations, regional networks, and private sector actors, in shaping global cybersecurity governance. Third, the study of international cybersecurity policy diffusion can help identify collaboration and coordination opportunities among countries and develop strategies for addressing the global nature of cybersecurity threats. Finally, by analyzing the diffusion of cybersecurity policies, scholars and policymakers can gain a deeper understanding of the broader dynamics of policy diffusion, including the mechanisms of influence and the factors that facilitate or hinder the adoption of policies across countries and regions.

Drivers of Global Cybersecurity Strategy Diffusion

We view the global adoption of national cybersecurity strategies as a process of diffusion, defined as a "prior adoption of a trait or practice in a population [that] alters the probability of adoption for remaining non-adopters" (Strang, 1991, 325). Taking this into account, the article explains the sequential decisions to adopt national cybersecurity strategy by followers or non-adopters.

Such sequential decisions have been of interest to policy diffusion scholars for decades. Starting with the focus on the adoption of state-level policies, mostly within the United States (Crain, 1966; Walker, 1969; Gray, 1973; Berry and Berry, 1990*b*,*a*), scholars have recently shifted to explain the global diffusion of liberal economic ideas (Simmons and Elkins, 2004), bilateral investment treaties (Elkins, Guzman and Simmons, 2006), human trafficking laws (Simmons, Lloyd and Stewart, 2018), and technological and military innovation (Pennings and Harianto, 1992; Robertson, Swan and Newell, 1996; Bitzinger, 1994), just to name a few. Examining the global diffusion of cybersecurity strategies, prior research points to the threat environment as the primary motivation (Azmi, Tibben and Win, 2016; Dunn-Cavelty, 2005; Lehto, 2013; Luiijf, Besseling and De Graaf, 2013).

To explain the global diffusion of cybersecurity strategies, we supplement existing explanations identified in the literature with anecdotes collected from reviewing primary and secondary sources, including but not limited to national cybersecurity strategy, policy briefs, testimonies and speeches by government officials. We have identified three potential drivers that can explain the global diffusion of national cybersecurity strategy—threats, international organizations, and common culture and language. We discuss each of these drivers below.

Explanation #1: Threat Environment

Prior studies explored the role of threats in driving policy adoption across various issues, including climate change, criminal law, environment, and energy policy (Duxbury, 2021; Steves and Teytelboym, 2013; Simmons, Wilson and Dean, 2021; Stern, Dietz and Vandenbergh, 2022; Hartmann et al., 2013). Cybersecurity policy is not an exception. Craig and Valeriano (2016), for instance, demonstrate that states are likely to make changes to their cybersecurity policies in reaction to cyber-threats. Valeriano and Maness (2015) discuss how cyber threat is a popular tool politicians use to motivate policy change.

Anecdotal evidence from policy documents provides further support for threats as explanations. For example, the UK has recognized the potential cyber threats posed by Russia and China and has implemented measures to strengthen its cybersecurity (Aitken, 2022; Faulconbridge, 2021). Similarly, the accusations of conducting cyber-attacks by Israel and Iran have motivated both countries to implement changes in their approach to cyber policies. Israel has bolstered its digital defenses to counter the perceived threat from Iran, while Iran improved its cybersecurity capabilities to protect against further attacks from Israel (Claridge, 2022; Al-Sarihi, Soliman and Jalal, 2023; Ahronheim, 2022; Bybelezer, 2022).

Combating cyberthreats was a key driver of cyber policy diffusion among the states of the Arab Convention, also known as the Convention on Combating Information Technology Offenses, signed in December 2010 by the Arab League. In line with this convention, member-states have made significant efforts towards implementing cybersecurity strategies to tackle cyberthreats and protect their respective nations' cyberspace. Text of these national cybersecurity strategies that point to cyber threats as a motivation behind the strategy adoption provides further anecdotal evidence for the threat environment explanation. Saudi Arabia, for instance, prioritizes its readiness for threat actors and technologies and recognizes the necessity of strengthening the Kingdom's overall cybersecurity in response to cyber threats (Saudi Arabian Monetary Authority, 2017). Similarly, Qatar's strategy focuses on threat responses and reviews existing capabilities to meet threats (Ministry of ICT, 2014). *Hypothesis 1* below summarizes our threat environment explanation.

> ***Hypothesis 1 (Threats):*** *Countries are more likely to adopt their national cybersecurity strategies in the years after they experienced cyber-threats.*

Explanation #2: Influence of International Organizations

While the above examples provide anecdotal support for the threat environment explanation, they also suggest that countries might be learning from each other through their membership in international organizations. Prior research shows that the exchange of information among connected actors is a driving force behind diffusion of various sociological processes (Axelrod, 1997; Rogers, 1995*a*). When it comes to the diffusion of innovation, international organizations facilitate the diffusion at a lower cost because such membership can allow states to quickly acquire necessary knowledge and expertise from other members who have already adopted this innovation.

In the cyber realm, cooperation through international organizations can facilitate ″economies of scale” when it comes to creating a cybersecurity “rulebook” that all nations can use to ensure that all members gain access to expert advice. This can help standardize best practices and create a common language for cybersecurity policies, possibly improving communication and coordination between nations. Additionally, international organizations can provide expert advice to member countries, ensuring that all members have access to the latest cybersecurity expertise and resources. By working together in this way, nations can, therefore, minimize the cost per country when drafting their original cybersecurity policies by relying on common resources.

The Organization of American States is a vivid example of where the information exchange regarding cybersecurity takes place, increasing the likelihood that OAS members adopt its first national cybersecurity strategy. For example, in 2004, the OAS developed a regional cybersecurity strategy with the goal of a multidimensional approach to creating a culture of cybersecurity. In addition, the OAS Inter-American Committee Against Terrorism (CICTE) created a specific cybersecurity program for the region meant to help states develop and implement a national cybersecurity strategy (Organization of American States, 2024). While the regional strategy serves as a rulebook, the cybersecurity program provides access to resources allowing countries to adopt their national cybersecurity strategies which follow this rulebook.

Besides developing a rulebook, the OAS has been visiting its member-states to help them develop its national cybersecurity strategies, including the governments of Colombia, Panama, and Trinidad and Tobago. In 2014, for instance, the OAS concluded a two-day event in Kingston in collaboration with the government of Jamaica, during which they helped the government to draft its first national cybersecurity strategy. Besides visiting states, the OAS also brings country experts together with the goal of helping them acquire new knowledge, which they can then use to develop national cybersecurity strategies back home. To achieve this goal, in 2017, Canada signed a multi-million dollar project with the OAS to enhance the cybersecurity skills of national entities (Organization of American States, 2017). Given this OAS involvement, as of 2020, eighteen countries from Latin America and the Caribbean made significant strides towards establishing officially recognized cybersecurity strategies (Bianchi, 2022). *Hypothesis 2A* below summarizes our international organizations explanation.

> ***Hypothesis 2A (Influence of International Organizations):*** *Countries are more likely to adopt their national cybersecurity strategies if they are members of international organizations.*

However, not all organizations are likely to have an equal impact on the cybersecurity adoption process. The above examples show that international alliances might be particularly relevant, given nations' desire to address transnational cybersecurity threats collectively. Prior literature points to an important role allies play in policy areas, such as environmental, technology and social policy, by sharing necessary knowledge required for policy adoption with their partners (Elkins, Guzman and Simmons, 2006; Long, Nordstrom and Baek, 2007; True and Mintrom, 2001; Saikawa, 2013; Kifle, Mbarika and Bradley, 2006). Alliances also matter when it comes to cybersecurity (Kostyuk, 2024, 2020). Kostyuk (2024), for instance, illustrates that allies with military cyber capabilities often assist their partners who lack these skills by sharing knowledge and expertise through training programs often tailored to address the specific needs and gaps identified in their partner nations, helping them build more resilient cyber defense systems. Moreover, alliances facilitate hands-on workshops where experts from various fields collaborate to develop innovative strategies and solutions to counter cyber threats (King, 2014; ENISA, 2024; UNIDIR, 2024).

Given that the adoption of the first national cybersecurity strategy marks the first public and main (national) effort that national leaders take to develop defensive responses to cyberthreats, we argue that the influence of allies in the cybersecurity strategy adoption might be particularly relevant. Therefore, we hypothesize that allies who already developed their national cybersecurity strategies are likely to assist their partners without such strategies to develop strategies of their own (*Hypothesis 2B*).

> ***Hypothesis 2B (Influence of Allies):*** *Countries are more likely to adopt their national cybersecurity strategies when their allies have already adopted such strategies.*

Explanation #3: Influence of Common Culture and Language

Culture and language can significantly affect the diffusion of innovation (Rogers, 1995*b*; Berry and Berry, 1990*a*,*b*). Cultural and linguistic similarities between nations can also facilitate policy transfer and diffusion because countries often learn from the successes and failures of culturally similar nations that have already implemented similar policies (Simmons and Elkins, 2004).

Cultural and linguistic affinities can significantly impact the diffusion of cybersecurity policies. When countries share common cultural backgrounds and linguistic ties, it becomes more straightforward for them to review and understand the policies of their counterparts. This mutual understanding fosters a smoother exchange of cybersecurity strategies and best practices among nations. Doing so ensures that there is no misinterpretation of various cybersecurity terms, which may differ between countries. For instance, some countries use the term ″information security″ to emphasize the confidentiality, integrity, and availability of information. Simply replacing ″information security″ with ″cybersecurity,″ which refers to the security of Internet-connected devices, in a national cybersecurity strategy could lead to the inability to execute the defense plan proposed by the country and give misleading signals to domestic and international audiences.

The influence of shared culture and language was evidence in the diffusion of cybersecurity strategies within the former Soviet Union bloc of countries. Following Russia's 2000 Doctrine of Information Security, cybersecurity strategies of these nations largely integrate Moscow's "information security" approach. Belarus, for instance, has included the Internet as a potential threat to ″information security″ in its law since 2001. Ukraine's 2009 Doctrine of Information Security defined its scope broadly to cover the protection of individual, societal, and state interests against incomplete, untimely, or unreliable information. Uzbekistan's 2002 Law on Principles and Guarantees on Access to Information permitted the government to restrict individuals' information access if it was deemed necessary to protect them from negative psychological influence and to counteract threats to information security, terrorism, and religious extremism.

> ***Hypothesis 3 (Influence of Common Culture and Language):*** *Countries are more likely to adopt their national cybersecurity strategies when their culturally similar nations have already adopted such strategies.*

Data & Empirical Strategy

Dependent Variable. Our dependent variable is the adoption of the first general, government-wide, national cybersecurity strategy (`Adoption`) during the 1999-2018 period. Countries are coded as a "1" if they enacted such a strategy and "0" if they have not done so during the studied period. To create this variable, we have collected a highly comprehensive data set of national cybersecurity strategies (National Cybersecurity Policies Data (NCSPD) (v1.0)). To ensure that our sample includes only the most relevant documents, we used the official government websites to collect the majority of the documents and followed a well-established practice in conflict studies by using multiple sources to record an event (Woolley, 2000). Specifically we consulted the databases of national cybersecurity strategies created by international organizations, such as the International Telecommunications Union, NATO Cooperative Cyber Defence Centre of Excellence, and the United Nations Institute for Disarmament Research. In some cases, we consulted country experts. Ninety-seven out of 160 nations included into this analysis adopted their first national cybersecurity strategies during the studied time.[1] Figure 2 displays the global spread of cybersecurity strategy during the four five-year periods.

Main Predictors. Since we have three potential explanations of the cybersecurity strategy diffusion, here we explain how we measure each of these explanations. First, we measure cyber-threats by the cumulative number of large, known cybercampaigns[2] that a country experienced in all years preceding its strategy adoption (`Total Cyber-attacks`).[3] To create this variable, we use Valeriano, Jensen and Maness 2018's Dyadic Cyber Incident Dataset (DCID) (v1.5)—one of the few available datasets on major, known cybercampaigns.[4] We also consider number of additional measures of a country's threat envi-

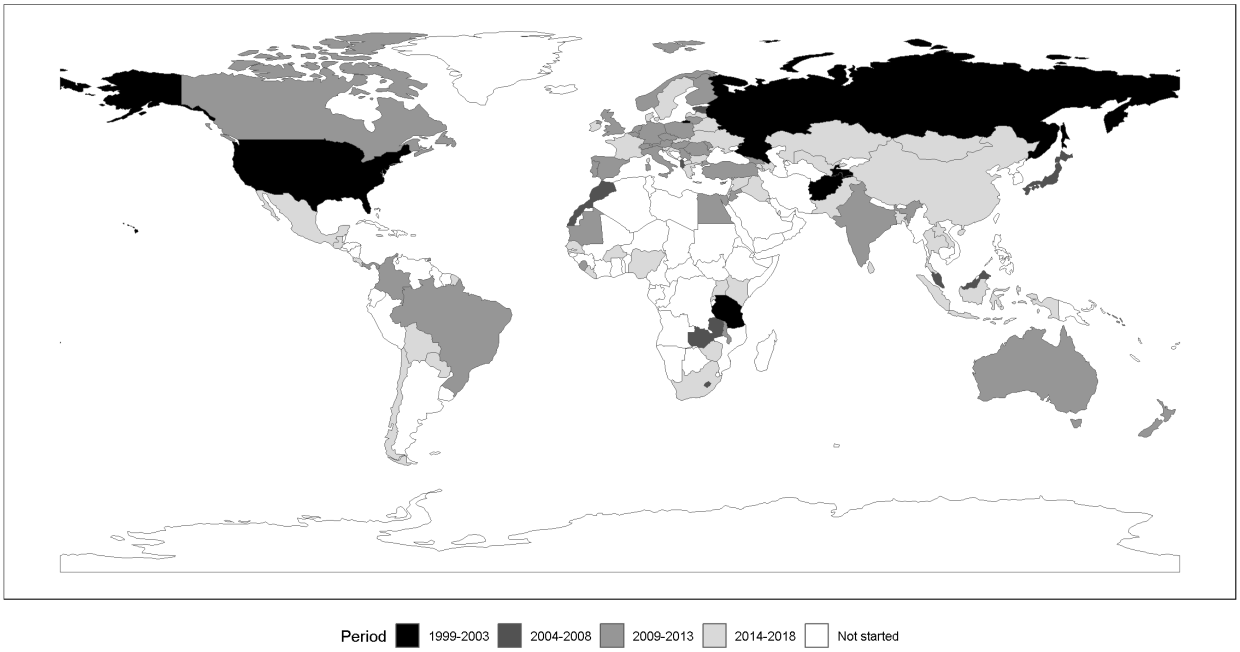
[1] Due to missing data in some covariates, some countries did not make to the final sample.

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

[3] 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.

[4] The Council on Foreign Relations' Cyber Operations Tracker (COT) is another data set that tracks cyberoperations. But since the majority of cyberincidents in the COT data depicts non-state cyberoperations or cases of governments using spyware to track actions of opposition leaders, this data is less suited for this project. *Source:* https://www.cfr.org/interactive/cyber-operations. Online Appendix provides a detailed

Figure 2: *Diffusion of National Cybersecurity Strategies (1999-2018)*



Source: National Cybersecurity Policies Data (NCSPD) (v1.0) collected by the one of the authors.

ronment (See Robustness Checks in the Online Appendix).

Second, we measure the influence of international organizations (IGOs) using Pevehouse et al. (2019)'s dataset that records each country's average membership in IGOs (`IGO Membership`). `Strategies adopted by allies` accounts for the influence of cybersecurity strategies adopted by allies. To identify allies, we use Leeds et al. (2002)'s Alliance Treaty Obligations and Provisions (ATOP) data because it contains a more detailed and comprehensive account of the studied period. We use the NCSPD dataset (v1.0) to identify which of these allies adopted their strategies prior to the time when a country adopts a strategy of its own.

Third, to account for the influence of culturally similar nations, we create a variable that captures the impact of strategies adopted by the country's cultural partners—nations that share the same culture and language (`Strategies adopted by cultural partners`).

explanation of DCID and its limitations, explaining why it is suitable for this analysis.

To identify cultural similar nations, we use two variables: (1) a binary variable that records whether the two nations have the same official language from Graham and Tucker (2019) (`Linguistic Partners`), and (2) a binary variable that records whether they have similar colonial experiences from Graham and Tucker (2019) (`Colonial Partners`). We use the NCSPD dataset (v1.0) to identify which of these cultural partners adopted their strategies prior to the time when a country adopts a strategy of its own.

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`).[5] 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`).[6] 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 1, if this score is at least six, which represents a democracy (`Democracy`).[7]

Method. We use an event history model[8] that focuses on the spell of time until the adoption of a national cybersecurity strategy occurs. Specifically, we employ a Cox Proportional-Hazards (CPH) model which tests for conditions that create a greater risk of the country

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

[6] We use a logarithmic transformation to address this variable's skewness. Since `GDP per Capita` and `Internet Users` are highly correlated (83%), we only include `Internet Users` into our analysis. But we include models with both variables in our robustness checks in the Online Appendix.

[7] We also use two additional cut-off points: nations that score a "5" or above receive a "1" (i.e., democracy) and those nations that score a "4" or below receive a "0" (i.e., autocracy). The obtained results remain fairly consistent.

[8] Event history models became a common tool for studying policy diffusion (Berry and Berry, 1990*a*; Elkins, Guzman and Simmons, 2006; Simmons and Elkins, 2004; Simmons, Lloyd and Stewart, 2018).

adopting its first cybersecurity strategy.[9] Our unit of analysis is the country-year. The analysis begins in 1999 shortly after the Internet became an international commercial network around that time, at least in Western Europe and the U.S. The analysis ends in 2018. If the country has not adopted a cybersecurity strategy by December 31, 2018, 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 international organizations overall, as well as network of formal alliances in particular, most consistently explain the global diffusion of national cybersecurity strategies. Tables 1 and 2, which present the results, shows positive statistically significant associations between `IGO Membership` and `Adoption`, as well as `Strategies adopted by allies` and `Adoption` with hazard ratios consistently larger than one.[10] Below, we review these findings in details.

We start with considering the threat environment as a plausible mechanism of the cybersecurity diffusion. Specifically, we consider the influence of the cumulative number of large cybercampaigns executed against the country in all years preceding its strategy adoption (`Total cyber-attacks`). Model 1 which displays the results demonstrates that `Total Cyber-attacks` have no statistically significant association with `Adoption` (HR: 1.03; CI: (0.93, 1.15)). These results do not support earlier findings that cyberthreats drive the diffusion of national cybersecurity strategies (Gomez, 2016) and refute *Hypothesis 1*.

We next examine the influence of international organizations as a driver of the global diffusion of cybersecurity strategies. Model 2 presents the results for the influence of

[9] Online Appendix provides a detailed explanation of the Cox Proportional-Hazards model, its assumptions, and various diagnostic tests.

[10] We use hazard ratios to present my 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	**International Organizations**	
	Model 1	*Model 2*	*Model 3*
Total Cyber-attacks (lag, sc)	1.03 (0.93; 1.15)	——	——
IGO Membership (lag, sc)	——	1.33** (1.18; 1.59)	——
Strategies adopted by allies (lag, sc)	——	——	1.25** (1.06; 1.47)
Democracy	1.82* (1.15; 2.89)	1.92* (1.21; 3.04)	1.81* (1.14; 2.86)
Internet Users per capita (log, sc)	2.19*** (1.53; 3.12)	2.27*** (1.59; 3.23)	2.22*** (1.55; 3.16)
Concordance	0.69	0.71	0.69

Note: This table focuses on the drivers of the global diffusion of national cybersecurity strategies, focusing on threats and international organizations (IGOs). It shows that the membership in IGOs and the influence of strategies adopted by a country's allies are likely to contribute to this diffusion whereas threats are unlikely to contribute to this trend. Results are from a Cox Proportional-Hazards model. Hazard ratios larger than 1 identify positive correlation and those smaller than 1 identify negative correlation. There are 2,470 observations and 94 events. All variables but `Democracy` are standardized. All results are based on two-tailed tests. Models with `Int_Users` do not include `GDP_PerCapita` because the two variables are highly correlated. `log:` logarithmized; `lag:` lagged; `sc:` standardized. $^{\wedge}p<0.1$; $^{*}p<0.05$; $^{**}p<0.01$; $^{***}p<0.001$

Table 2: *Explaining the Global Diffusion of National Cybersecurity Strategies (hazard ratios and confidence intervals)*

	Influence of cultural partners		**Model w/ all explanations**
	Model 4	*Model 5*	*Model 6*
Strategies adopted by colonial partners (lag, sc)	0.86 (0.73;1.00)	——	0.83* (0.70; 0.98)
Strategies adopted by linguistic partners (lag, sc)	——	1.01 (0.90; 1.13)	0.99 (0.88; 1.11)
Total Cyber-attacks (lag, sc)	——	——	1.07 (0.97; 1.18)
IGO Membership (lag, sc)	——	——	1.24* (1.02; 1.50)
Strategies adopted by allies (lag, sc)	——	——	1.26* (1.06; 1.51)
Democracy	1.99** (1.25; 3.16)	1.67* (1.05; 2.67)	1.94** (1.20; 3.12)
Internet Users per capita (log, sc)	2.19*** (1.54; 3.12)	1.99*** (1.39; 2.85)	1.95*** (1.36; 2.80)
Concordance	0.706	0.692	0.714

Note: This table focuses on the drivers of the global diffusion of national cybersecurity strategies, focusing on the effect of cultural partners primarily. We measure 'culture partners' by the common colonial past or common official language. The results show that the influence of strategies adopted by a country's colonial partners are likely to contribute to this diffusion. Results are from a Cox Proportional-Hazards model. Hazard ratios larger than 1 identify positive correlation and those smaller than 1 identify negative correlation. There are 2,470 observations and 94 events. All variables but `Democracy` are standardized. All results are based on two-tailed tests. Models with `Int_Users` do not include `GDP_PerCapita` because the two variables are highly correlated. `log:` logarithmized; `lag:` lagged; `sc:` standardized. $^{\wedge}p<0.1$; $^{*}p<0.05$; $^{**}p<0.01$; $^{***}p<0.001$

the membership in international organizations as a strategy driver. A positive, statistically significant correlation between IGO Membership and Adoption (HR: 1.33; CI: (1.18, 1.59)) suggests that the membership in IGOs is likely to contribute to the diffusion of national cybersecurity strategies. Model 3 examines a particular subset of international organizations—international alliances—and show that they are likely to contribute to the diffusion of national cybersecurity strategies. In particular, Strategies adopted by allies are positively and statistically significantly correlated with Adoption (HR: 1.25; CI: (1.04, 1.51)).

Additionally, we examine the influence of culturally similarly nations. Model 4 presents the results for the influence of nations that share the same colonial past who might still have lots in common (e.g., former British colonies in Africa). It shows no statistically significant relationship between Strategies adopted by colonial partners and Adoption (HR: 0.86; CI: (0.73, 1.00)). Model 5 uses a different measure of culturally similar nations—nations that share the same language. It shows no statistically significant relationship between Strategies adopted by linguistic partners and Adoption (HR: 1.01; CI: (0.90, 1.13)). Together results demonstrate that culturally similarly nations are unlikely to driver the global diffusion of cybersecurity strategies.

Last, we include Model 6 that contains all predictors. We observe a positive and statistically significant correlation between IGO Membership and Adoption (HR: 1.24; CI: (1.02, 1.50)), as well as between Strategies adopted by allies and Adoption (HR: 1.26; CI: (1.06, 1.51)). While coefficient on Strategies adopted by colonial partners is statistically significant, the hazard ratios are smaller than one (HR: 0.83; CI: (0.70, 0.98)), identifying a negative association. This result suggests that if a country's colonials partners adopted their national cybersecurity strategies this year, the country is less likely to adopt its own strategy next year. Together, the results presented in Model 6 further provides support for *H2A* and *H2B* and suggest that we should refute *H3*.

Robustness Checks. Our main findings that international organizations are likely to contribute to the strategy diffusion are also robust to: (1) alternative network specifications (neighbors); (2) an alternative measures of threats; (3) an alternative model specification (generalized linear models); and (4) an alternative functional form of the covariates (the inverse hyperbolic sine function) (see Robustness Checks in the Online Appendix).

Discussion

We examine the diffusion of cybersecurity policies across the world and ask a basic question: *what drives the diffusion of cybersecurity policy?* We explore several alternative explanations that are common in the literature on policy diffusion and find that nations follow their allies when they adopt their national cybersecurity strategy.

Our study contributes to the literature on cybersecurity policy highlighting that contrary to the few existing works demonstrating that a country's cyberthreat environment being a driver (Gomez, 2016), international organizations, as well as international alliances are what motivates countries to develop new policies related to cybersecurity. While the threat environment undoubtedly plays a role, our findings underscore the importance of shared interests, values, and strategic cooperation among allies.

Our results challenge the threat-centric view, indicating that countries can take the route of cooperation, adopting and shaping their cybersecurity policies in line with shared interests. Recognizing that cooperation is the driving force for cybersecurity policy diffusion underscores the preventive character of such strategies, suggesting that nations are increasingly looking to build resilience through partnerships rather than relying solely on reactive measures.

Several reasons could be behind choosing collaboration over response to threat. For one, countries might recognize that cyber threats are often transnational and that isolated responses are less effective than coordinated ones. Another reason could be that assessing the cyber threat environment can be challenging due to its complexity and the rapid evolution of threats. As a result, countries might find it more straightforward to align with allies' strategies than to continuously reassess their threat landscapes. Third, there may be shared benefits to cooperation that outweigh the benefits of responding individually to threats. By pooling resources and knowledge, countries can develop more comprehensive cybersecurity capabilities than they could alone. Broadly speaking, the emphasis on cooperation in cybersecurity policy diffusion could be indicative of a broader shift towards more collaborative forms of technology governance. This could have implications for how countries collaborate on challenges related to emerging technology, emphasizing the need for collective expertise, shared responsibility, and mutual benefit.

When it comes to policy implications, this study reveals that international organizations and allies are likely to play an important role in influencing a nation's decision to adopt its first national cybersecurity strategy, marking the initiation of its state cybersecurity apparatus. This influence can extend beyond the initial adoption, likely shaping the entire trajectory of the nation's cybersecurity policies and practices. Through shared interests and strategic cooperation, IGO's and allies seem to be guiding not only the formulation of initial strategies but also the ongoing development and coordination of the cybersecurity framework. Their impact resonates throughout the entire spectrum of cybersecurity governance, reflecting an interconnected global landscape.

Moreover, it is possible that the influence of IGO's and allies in shaping cybersecurity policies will grow in significance with the rapid advancement of technology. As the impact of ICTs and the Internet expands into every aspect of our lives, the complexity and scope of cybersecurity challenges are set to increase exponentially. This escalating complexity necessitates a solidified and coordinated approach within international organizations and among allies. Their influence can be expected to become an essential pillar in shaping the global cybersecurity landscape, transcending mere collaboration to form a unified front. By fostering innovation, sharing intelligence, and coordinating responses, international organizations and alliances can be instrumental in building a resilient and secure digital future. In a world where technology is evolving at an unprecedented pace, this collaborative behavior among countries can be a defining factor. It can determine how nations adapt to these changes and thrive in this intricate and rapidly changing technological landscape.

This research takes the first stab at an important and novel area of scientific inquiry. Our findings serve as a useful point of departure not only for international relations scholars but for political scientists in general. We focus on the policy innovation—an adoption of the first strategy—because its diffusion is a new phenomenon[11] but future research should explain future policy expansion.

Future research could account for different types of cybersecurity documents issued by the government. While this study focuses on cybersecurity strategies, other prevalent types of documents include digital agendas, e-government strategies, ICT policy documents, as well as national cyberdefense strategies. Studying content of these documents and determining whether there are differences or similarities in the content of these documents among countries could offer insights into how cybersecurity concerns and priorities are framed and addressed globally. This comparative analysis could reveal common threads and divergent approaches across nations. For example, identifying whether certain themes, such as privacy, data protection, or cybercrime prevention, are emphasized

[11] Only ninety-seven nations adopted their first strategy and only twenty-eight nations updated their strategy.

similarly or differently across types of documents and countries could highlight global cybersecurity trends or regional specificities. Moreover, examining the content of these varied documents could help in understanding the influence of international cybersecurity standards and frameworks on national policies, as well as how countries adapt these global norms to fit their local context and security needs. This future work could uncover the role of geopolitical, economic, and technological factors in shaping the cybersecurity strategies of different nations, providing a more nuanced understanding of the diffusion process.

This research makes the following contributions to the political science literature. While most existing works in cybersecurity literature focus on competition between the great powers and how they acquire military cybercapacity (Borghard and Lonergan, 2017; Gartzke, 2013; Nye Jr, 2017; Valeriano, Jensen and Maness, 2018), we instead seek to explain the strategic behavior of weaker cyber states and the ways they address their cyber vulnerabilities. Even though cybersecurity strategies are softer defensive measures and do not send as strong of a signal as military capabilities, they are still important because they mark the initiation of a state cybersecurity apparatus. Since nations learn from their allies when they start creating this apparatus as our results show, these partners will influence how nations continue to build their apparatuses, including doctrines that define their conduct in cyberspace and the types of capabilities they develop to achieve their strategic goals.

This article makes a contribution to international relations literature by examining the motivations that lead to adoptiong of cybersecurity strategies across the world. By providing the first systematic account of the spread of cybersecurity strategies as an example of policy innovation, this article seeks to understand the motives behind cybersecurity strategy creation in order to form a better understanding of the strategies that shape the national information and communications technology (ICT) environment. By introducing highly comprehensive[12] cross-national time-series data on national cybersecurity strategies that serve as a proxy of countries' first and basic defensive cybercapabilities, this research serves as an important stepping stone for future research on the causes and effects of state cybercapacity.

This research makes a contribution to a broader political science literature by helping us better understand how policies diffuse in the information age. As actors attempt to navigate the complex network of international organizations, regional networks, and private sector actors, the growing interconnection of the global community has produced new obstacles and opportunities for policy diffusion. By looking at the elements that influence policy dispersion in the cybersecurity sector, we can better understand how policies disseminate more generally in the information age, especially in areas like privacy, data protection, and internet governance. As policymakers attempt to solve the complicated and linked issues of the digital era, this insight may have ramifications for a variety of policy areas outside cybersecurity.

[12] The second most comprehensive, published data set includes only 64 strategies from 54 countries, covering the 2003-2015 period (Azmi, Tibben and Win, 2016).

References

Abdullah, Fazlan, Nadia Salwa Mohamad and Zahri Yunos. 2018. "Safeguarding Malaysia's cyberspace against cyber threats: contributions by cybersecurity Malaysia." *OIC-CERT Journal of Cyber Security* 1(1):22–31.

Aggarwal, Vinod K and Andrew W Reddie. 2018. "Comparative industrial policy and cybersecurity: the US case." *Journal of Cyber Policy* 3(3):445–466.

Ahronheim, Anna. 2022. "Israel has foiled dozens of cyber attacks by Iran over last year, IDF.".
URL: *https://www.jpost.com/israel-news/article-717786*

Aitken, Peter. 2022. "UK tightens security over hacking fears from Russia, China.".
URL: *https://www.foxnews.com/world/uk-tightens-security-hacking-fears-russia-china*

Al-Sarihi, Aisha, Mohammed Soliman and Ibrahim Jalal. 2023. "Israel's new Iran Strategy Complicates Regional Security.".
URL: *https://www.mei.edu/publications/israels-new-iran-strategy-complicates-regional-security*

Axelrod, Robert. 1997. "The dissemination of culture: A model with local convergence and global polarization." *Journal of conflict resolution* 41(2):203–226.

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*a*. "State lottery adoptions as policy innovations: An event history analysis." *American political science review* 84(2):395–415.

Berry, Frances Stokes and William D Berry. 1990*b*. "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*

Bitzinger, Richard A. 1994. "The globalization of the arms industry: The next proliferation challenge." *International Security* 19(2):170–198.

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

Bybelezer, Charles. 2022. "Iran blames Israel for Fars News Agency hack.".
URL: *https://www.jns.org/iran-blames-israel-for-fars-news-agency-hack/*

Catota, Frankie E, M Granger Morgan and Douglas C Sicker. 2019. "Cybersecurity education in a developing nation: the Ecuadorian environment." *Journal of Cybersecurity* 5(1):tyz001.

Cheung, Tai Ming. 2018. "The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities." *Journal of Cyber Policy* 3(3):306–326.

Claridge, David. 2022. "Israel bolsters digital defense amid Iran Cyber threat.".
URL: *https://www.geopoliticalmonitor.com/israel-bolsters-digital-defense-amid-iran-cyber-threat/*

Craig, Anthony and Brandon Valeriano. 2016. "Securing Cyberspace: The Drivers of National Cyber Security Policy." *Presented at the International Studies Association Conference* .

Crain, Robert L. 1966. "Fluoridation: the diffusion of an innovation among cities." *Social Forces* 44(4):467–

476.

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

Duxbury, Scott W. 2021. "Who controls criminal law? Racial threat and the adoption of state sentencing law, 1975 to 2012." *American Sociological Review* 86(1):123–153.

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

ENISA. 2024. "Cyber Security Strategy in Sweden – work in progress.".
URL: *https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshops/SwedishNCSS.pdf*

Faulconbridge, Guy. 2021. "UK to help vulnerable countries against Russia, china cyber threat.".
URL: *https://www.reuters.com/technology/uk-help-vulnerable-countries-against-russia-china-cyber-threat-2021-05-12/*

Gartzke, Erik. 2013. "The myth of cyberwar: bringing war in cyberspace back down to earth." *International Security* 38(2):41–73.

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

Graham, Benjamin AT and Jacob R Tucker. 2019. "The international political economy data resource." *The Review of International Organizations* 14(1):149–161.

Gray, Virginia. 1973. "Innovation in the states: A diffusion study." *American political science review* 67(4):1174–1185.

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* .

Hartmann, Patrick, Vanessa Apaolaza, Clare D'Souza, Carmen Echebarria and Jose M Barrutia. 2013. "Nuclear power threats, public opposition and green electricity adoption: Effects of threat belief appraisal and fear arousal." *Energy Policy* 62:1366–1376.

Huang, Hsini and Tien-Shen Li. 2018. "A centralised cybersecurity strategy for Taiwan." *Journal of Cyber Policy* 3(3):344–362.

InternationalTelecommunicationsUnion. 2010. "Guide to Developing a National Cybersecurity Strategy." *International Telecommunication Union* .

Johnsen, S. 2015. "A comparative study of the Norwegian cyber security strategy vs. strategies in the EU and US–Emerging cybersafety ignored." *Safety and Reliability of Complex Engineered Systems, L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio and W. Kroger (Eds.), CRC Press/Balkema, Leiden, The Netherlands* pp. 3485–3492.

Kifle, Mengistu, Victor WA Mbarika and Randy V Bradley. 2006. "Global diffusion of the internet x: the diffusion of telemedicine in ethiopia: potential benefits, present challenges, and potential factors." *Communications of the Association for Information Systems* 18(1):30.

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

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

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

Lehto, Martti. 2013. The ways, means and ends in cyber security strategies. In *Proceedings of the 12th European conference on information warfare and security*. pp. 182–190.

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.

Min, Kyoung-Sik, Seung-Woan Chai and Mijeong Han. 2015. "An international comparative study on cyber security strategy." *International Journal of Security and Its Applications* 9(2):13–20.

Ministry of ICT, X. 2014. "Qatar National Cyber Security Strategy.".

Nye Jr, Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41(3):44–71.

Organization of American States, x. 2017. "Canada Commits Can2.5*milliontotheOAStoPromoteCybersecurityInitiatives*.″.
URL:

Online Appendix:
Data, Method, & Robustness Checks

"Role of International Organizations and Formal Alliances in Global Diffusion of National Cybersecurity Strategies"

Nadiya Kostyuk
Jen Sidorova
Georgia Institute of Technology

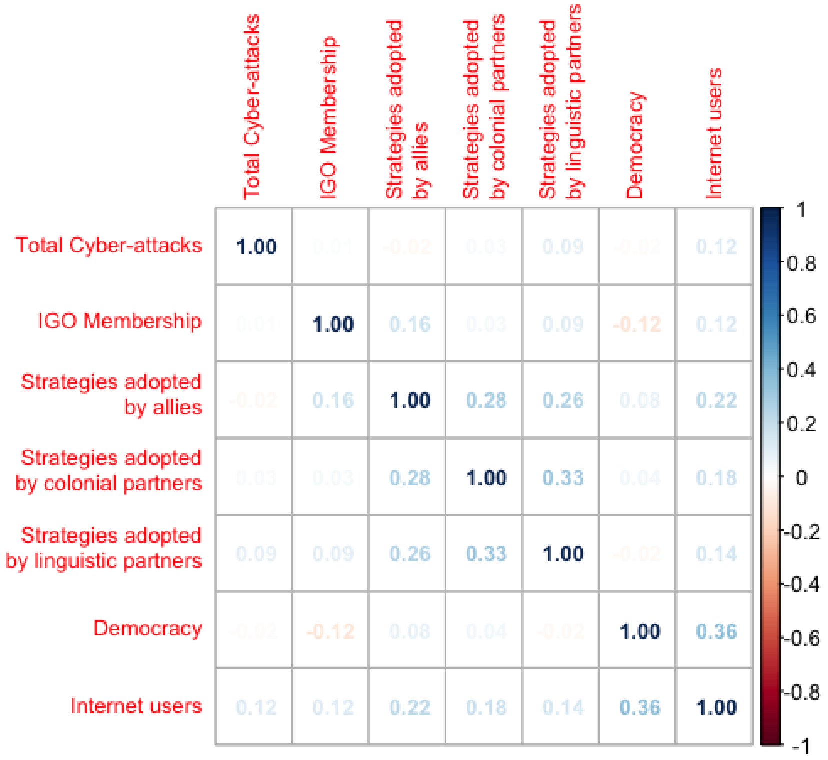
March 30, 2024

Contents

1 Summary Statistics

Figure 1 displays the correlation plot for the main explanatory variables. Table 3 shows the summary statistics for these variables and our outcome of interest. All variables besides `Democracy` have been re-scaled to make it easy to interpret the obtained results.

Figure 1: *Correlation Plot*



	Total Cyber-attacks	IGO Membership	Strategies adopted by allies	Strategies adopted by colonial partners	Strategies adopted by linguistic partners	Democracy	Internet users
Total Cyber-attacks	1.00	0.01	-0.02	0.03	0.09	-0.02	0.12
IGO Membership	0.01	1.00	0.16	0.03	0.09	-0.12	0.12
Strategies adopted by allies	-0.02	0.16	1.00	0.28	0.26	0.08	0.22
Strategies adopted by colonial partners	0.03	0.03	0.28	1.00	0.33	0.04	0.18
Strategies adopted by linguistic partners	0.09	0.09	0.26	0.33	1.00	-0.02	0.14
Democracy	-0.02	-0.12	0.08	0.04	-0.02	1.00	0.36
Internet users	0.12	0.12	0.22	0.18	0.14	0.36	1.00

Table 1: *Summary Statistics*

	Minimum	*Median*	*Mean*	*Maximum*
Adoption	0	0	0.04	1
Total Cyber-attacks (lag, sc)	-0.13	-0.13	0	25.26
Strategies adopted by adversaries (lag, sc)	-6.68	-0.09	0	6.37
IGO membership (lag, sc)	-3.19	-0.07	0	3.68
Strategies adopted by allies (lag, sc)	-0.34	-0.34	0	15.52
Strategies adopted by colonial partners (lag, sc)	-0.26	-0.26	0	6.58
Strategies adopted by linguistic partners (lag, sc)	-0.3	-0.3	0	14.65
Democracy	0	1	0.53	1
Internet Users (log,sc)	-1.73	0.11	0	1.57

Note: All variables but `Democracy` are standardized. `log:` logarithmized; `lag:` lagged; `sc:` standardized.

2 Empirical Strategy

2.1 Spatial lags

To identify the effect of the strategies adopted by a country's so-called "neighbors"[1] that include but are not limited to its allies, adversaries, and cultural partners, we create spatial lags. Instead of lagging the value of the dependent unit one variable at a time and, as a result, adding a significant number of regressors to my model, we use spatial lags that capture the "weighted average of the dependent variable in the actor's 'neighborhood"' (Simmons and Elkins, 2004, 178). We define a spatial lag for a country i as:

$$W_i([t-1]) * y_{-i}([t-1]) = \sum_{i=1,\ldots,N} W_{i,-i}([t-1]) * y_{-i}([t-1]), \tag{1}$$

where, $W_{i,-i}([t-1])$ is an $N \times N$ spatial weights matrix that capture's countries i's neighborhood in $t-1$. Each element in $W_{i,-i}$ measures various dispersion variables, explained in Section 3, between any two nations. For instance, it could measure physical distance between two nations' capitals, how much trade the two nations do, or whether they signed a military alliance treaty. $\sum_{i=1,\ldots,N} W_{i,-i}$ captures the weight of the relationship between these two nations relative to the nation's total relationships with other nations in a given area of international relations. This weight captures the importance of a neighbor's influence on this country. For instance, if a nation has only one trading partner, then their trading relationship has a weight of 100%; consequently, the partner will most likely have a significant influence on this country's economic decisions. On the other hand, if a nation has twenty trading partners and each relationship has a weight of 5%, then the influence of an individual trading partner on the country's economic decisions will most likely be limited. $y_{-i}([t-1])$ represents whether a country's "neighbor" $-i$ adopted a cybersecurity strategy in year $t-1$. Combined, $W_i([t-1]) * y_{-i}([t-1])$ captures the total effect of the country's "neighbors" that adopted or did not adopt cybersecurity strategies in $t-1$.

[1] I use this general concept of "neighbors" to refer to various types of networks through which strategies can diffuse.

2.2 Cox Proportional-Hazards model

Model explained. We fit the following Cox Proportional-Hazards (CPH) model that examines the effect of time-varying and time-invariant covariates on the country's decision to adopt the strategy:

$$log(H(t; X_i([t-1]), y_i([t-1]))) \propto W_i([t-1])y_{-i}([t-1])\beta_1 + X_i([t-1])\beta_2,$$

where: $log(H(t; X_i([t-1]), y_i([t-1])))$ is the log of a hazard ratio that stands for the relative risk of country i adopting a cybersecurity strategy at time t; $W_i([t-1])y_{-i}([t-1])$ is an $n \times n$ spatial weights matrix, as explained above; $X_i([t-1]) = [x_{1i}([t-1]), \ldots, x_{ki}([t-1])]'$ is a matrix of k exogenous variables; and β_2 is a three-dimensional vector of coefficients. As explained earlier, we included the following exogenous variables: (1) the country's regime type (`Democracy`); (2) the country's GDP per capita in a given year (`GDP per Capita`); and (3) the number of the country's Internet users as a percentage of its total population in a given year (`Internet Users per Capita`).[2] We also use robust standard errors with clustering on the countries to account for time-varying coefficients. Lastly, to make our results easy to interpret, we standardize all continuous explanatory variables (all variables except `Democracy`).

Non-proportionality assumption. One assumption of the CPH model is that no two countries adopt strategies at the same time. In practice, this is not necessarily the case. Many countries adopt strategies in the same year. To "break this tie," We used the Efron approximation in my model as it is a tighter approximation to the exact marginal. Another assumption of the CPH model is that the hazard ratios do not vary over time. This means that if a country's Internet dependency increases the probability that the country adopts a cybersecurity strategy by ten percent, this effect should remain the same in 2010 and 2020. In practice, however, this assumption is often not met. For instance, because citizens might be more aware of the impact of the Internet in 2020, the country's Internet dependency in 2020 might have a higher effect on its probability of the strategy adoption than in 2010. This results in a non-proportional hazard model (Box-Steffensmeier, Reiter and Zorn, 2003). One way to test this assumption is to use the Therneau and Grambsch non-proportionality test that uses scaled Schoenfeld residuals (Grambsch and Therneau, 1994). If any variable violates this assumption, we interact this variable with starting time (`tstart`) to address this issue (Therneau, Crowson and Atkinson, 2020). Despite following this recommendation by the authors of the R package, the effect of these variables should be generally understood as an average effect over the entire studied period and not as a conditional effect over a particular period of time.

While the Therneau and Grambsch non-proportionality test detects a number of specification errors in addition to non-proportionality, it may yield a false-positive test if the model is specified incorrectly (Therneau, Grambsch and Fleming, 1990; Grambsch and Therneau, 1994; Therneau and Grambsch, 2000). Thus scholars recommend improving the model specification for the correct functional form of the covariates (i.e., detect any non-linear fit). This could be done by either "including polynomial functions of variables or using a non-parametric method such as splines" (Keele, 2010, 192). Since polynomials may be "poor approximations for more complex linear functional forms" (Keele, 2010, 195), local form of estimation—splines—are used to model non-linearity (Beck and Jackman, 1998; Beck, Katz and Tucker, 1998; Ruppert, Wand and Carroll, 2003). Since in some circumstances it is difficult to use the splines, we use the inverse hyperbolic sine (IHS) function

[2] Models with `Internet Users per Capita` do not include `GDP per Capita` because the two variables are highly correlated.

instead (Shadden and Zorn, 2011).[3] We ran robustness checks where we use the inverse hyperbolic since function for continuous covariates. The results remain robust to this alternative function specification (Section 3.4).

Residual auto-correlation. Given that we use a *pure space-recursive model*, in which "the dependence pertains to neighboring locations in a different period" (Anselin, 2001, 13), residual auto-correlation could be an issue. To check for residual auto-correlation in the presence of spatially lagged dependent variables, we apply the Breusch-Godfrey test to my base model. The p-value of 0.978 confirms that we cannot reject my null hypothesis that residual auto-correlation (λ) is statistically significant from 0 ($H_0 : \lambda = 0$).

Identification issue. Identification issue—the inability, in principle, to identify the best estimate of the value(s) of a parameter/s in a model—is a known issue in diffusion models. Specifically, different choices of a spatial weight matrix, W, will result in different effect of strategies adopted by a country's neighbors, $W_i([t-1]) * y_{-i}([t-1])$. Even though network pre-specification is "one the biggest hurdles" in spatial analysis, we follow Betz, Cook and Hollenbach (2019, 1)'s recommendation and pursue spatial analysis even with limited information on network ties because a spatial model with a misspecified weights matrix still "weakly dominate[s] non-spatial models." Moreover, while Bayesian model averaging (BMA), which incorporates the uncertainty about specific network structure in empirical models, addresses this issue to some extent (Juhl, 2020), its purpose is slightly different from the goal of this study. BMA's main purpose is, first, to determine the best specification of a latent network by tuning small specifications of the same network and, then, to compare how they predict policy adoption. This article, instead, aims to explain how different types of networks explain strategy adoption. For instance, an BMA approach compares ten different specifications of a country's neighbors and decides which specification has the best model fit. This article, instead, aims to understand how in addition to the country's neighbors, its trading partners, military allies, and other actors affect the likelihood of the country's strategy adoption.

Homophily versus diffusion. The structure of international interaction—which alliances a country joins, which statements it makes in a forum like UNGA, etc.—is potentially endogenous to countries' interests, and their expectation of how others in the system will behave. Thus, one of the main questions in the diffusion analysis is: how can we differentiate between diffusion (i.e., social influence or contagion) and homophily (i.e., "formation on social ties due to matching individual traits" (Shalizi and Thomas, 2011, 211)) in these international networks? These phenomena are difficult to distinguish in purely observational studies. Precisely, Shalizi and Thomas (2011) demonstrate that these two phenomena are confounded with each other. Shalizi and Thomas (2011, 213) demonstrate that the identification of the contagion effect requires strong parametric assumptions and conclude, "contagion (diffusion) effects are nonparametrically unidentifiable in the presence of latent homophily—that there is just no way to separate selection from influence observationally" Shalizi and Thomas (2011, 216). As a result, differentiating between homophily and diffusion, if it is a network that is subject to selection effects, can only be done with an experiment (e.g., Fowler and Christakis (2010)).

[3] We considered using log-like functions but since the log function is not defined at zero, we used the inverse hyperbolic sine function, which looks like the log function but is defined at zero.

Table 2: *Robustness Checks: alternative network specification (hazard ratios and confidence intervals*

	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*
Strategies adopted by neighbors (1) (lag,sc)	1.02(0.92; 1.13)	——	——	——	——
Strategies adopted by neighbors (2) (lag,sc)	——	0.95(0.82; 1.09)	——	——	——
Strategies adopted by neighbors (3) (lag,sc)	——	——	1.24*(1.03; 1.51)	1.13(0.89; 1.42)	1.18(0.96; 1.45)
Strategies adopted by allies (lag,sc)	——	——	——	1.19^(0.99; 1.44)	——
IGO Membership (lag,sc)	——	——	——	——	1.3**(1.08; 1.55)
Democracy	1.8*(1.13; 2.85)	1.83**(1.16; 2.89)	1.75*(1.1; 2.78)	1.66*(1.04; 2.65)	1.92**(1.2; 3.06)
Internet Users per capita (log, sc)	2.2***(1.54; 3.14)	2.24***(1.57; 3.21)	2.03***(1.41; 2.91)	1.94***(1.35; 2.79)	2.05***(1.43; 2.94)
Concordance	0.69	0.69	0.69	0.69	0.71

Note: Results are from a Cox Proportional-Hazards model. Hazard ratios larger than 1 identify positive correlation and those smaller than 1 identify negative correlation. There are 2,470 observations and 94 events. All variables but `Democracy` are standardized. All results are based on two-tailed tests. $^{\wedge}$p<0.1; *p<0.05; **p<0.01; ***p<0.001

3 Robustness Checks & Additional Results

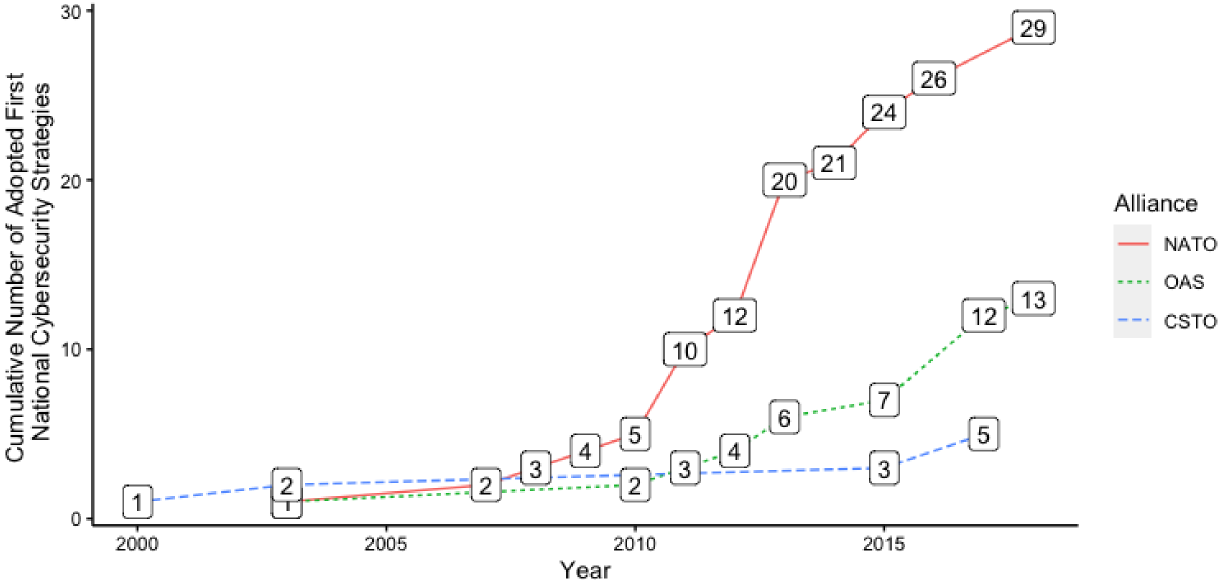
We conduct the following robustness checks:

1. alternative network specification (Section 3.1);
2. trends among alliances (Section 3.2);
3. alternative measures of threats (Section 3.3);
4. alternative functional form (Section 3.4); and
5. alternative model specification (Section 3.5).

3.1 Alternative network specification

The initiation of cybersecurity strategy by a country's geographic neighbors might motivate the country to develop its own strategy. We use the following 3 ways to identify a country's neighbors: (1) a dummy variable indicating whether states share a land border or are separated by less than 150 miles of water from Stinnett et al. (2002) (`Neighbors (1)`); (2) a dummy variable indicating whether states share a land border or are separated by less than 400 miles of water from Stinnett et al. (2002) (`Neighbors (2)`); and (3) a continuous variable that records the distance between the nations' capitals (`Neighbors (3)`). Models 1 through 5 in Table 2 which displays the obtained results shows that the adoption of national cybersecurity strategies by a country's neighbors is unlikely to be the primary explanation of the global cybersecurity strategy diffusion.

Figure 2: *Adoption of the first national cybersecurity strategies by different types of alliances (2000-2018)*



Source: Author's calculations based on the National Cybersecurity Policies (NCSP) data (version 1.0), collected by the author. Data on alliances collected by the author.

3.2 Trends among alliances

Our research reveals that membership in intergovernmental organizations (IGOs) influences the global diffusion of national cybersecurity strategies. Additionally, we observe diffusion occurring after alliances. As depicted in Figure 2, countries belonging to different alliances tend to adopt cybersecurity strategies at varying times. For instance, while countries in the Collective Security Treaty Organization initiated their adoption of cybersecurity strategies earlier, those in the North Atlantic Treaty Organization took the lead by 2010. To further explore the significance of a country's membership in different military alliances, we conducted additional tests, the results of which are presented in Table 3. These findings suggest that although membership in specific alliances, such as NATO, may have a greater impact, the strategies adopted by a country's allies also play a role in the diffusion process.

3.3 Alternative Measures of Threats

In addition to accounting for the actual threats that a country experienced, we also account for the possibility that the diffusion after adversaries can take place. This is because the development of strategies can be an indirect proxy for the development of capabilities. To account for that possibility, we record a weighted average effect of cybersecurity strategies adopted by the country's adversaries in a period prior to the country adopting its first cybersecurity strategy (`Strategies`

Table 3: *Robustness Checks: alliance trends (hazard ratios and confidence intervals*

	Model 1	*Model 2*	*Model 3*
Strategies adopted by allies (lag,sc)	1.17^(0.98; 1.41)	1.22*(1.04; 1.43)	1.23*(1.05; 1.45)
NATO Member	1.69^(0.92; 3.09)	——	——
OAS Member	——	0.52*(0.28; 0.93)	——
CSTO Member	——	——	1.42(0.55; 3.68)
Internet Users per capita (log,sc)	1.81**(1.24; 2.64)	1.98***(1.4; 2.8)	1.99***(1.39; 2.85)
Democracy	1.54^(0.95; 2.5)	1.85*(1.15; 2.97)	1.72*(1.07; 2.77)
Concordance	0.69	0.7	0.7

Note: Results are from a Cox Proportional-Hazards model. Hazard ratios larger than 1 identify positive correlation and those smaller than 1 identify negative correlation. There are 2,470 observations and 94 events. All variables but `Democracy` are standardized. All results are based on two-tailed tests. ^p<0.1; *p<0.05; **p<0.01; ***p<0.001

Table 4: *Robustness Checks (continued) (hazard ratios and confidence intervals)*

	Model 1	*Model 2*
	Threats	*Functional form*
Strategies adopted by adversaries (lag,sc)	1.03(0.9; 1.18)	——
Strategies adopted by allies (lag,sc)	——	1.49**(1.11; 2)
Internet Users per capita (log,sc)	2.2***(1.54; 3.14)	2.22***(1.44; 3.44)
Democracy	1.82*(1.15; 2.88)	1.68*(1.06; 2.68)
Concordance	0.69	0.69

Note: Results are from a Cox Proportional-Hazards model. Hazard ratios larger than 1 identify positive correlation and those smaller than 1 identify negative correlation. There are 2,470 observations and 94 events. All variables but `Democracy` are standardized. All results are based on two-tailed tests. ^p<0.1; *p<0.05; **p<0.01; ***p<0.001

`adopted by adversaries`). We use Maoz (2005)'s data on Militarized Interstate Disputes (MID) to identify adversaries. We use the NCSPD dataset (v1.0) to identify which of these adversaries adopted their strategies prior to the time when a country adopts a strategy of its own. Since states can attack each other using cyber and/or conventional means, we identify adversaries using Diehl, Goertz and Gallegos (2021)'s Peace Data (v3.01)[4] DCID)(v1.5). The results in Model 1 in Tabl 4 also provide evidence that diffusion of cybercapacity is unlikely to take place after adversaries.

3.4 Alternative functional form

To investigate whether we employ the correct functional form of the covariates, we run robustness checks using the inverse hyperbolic sine function for continuous covariates. Model 2 in Table 4 demonstrates that the earlier obtained results generally hold. `IGO Membership` is statistically significant (HR: 1.44**(1.11; 1.88)).

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

Table 5: *Robustness Checks: alternative model specification (odds ratios and confidence intervals)*

	Model 1
Strategies adopted by allies (lag,sc)	1.318***(1.17, 1.48)
IGO Membership	1.220^(0.97, 1.53)
Internet Users per capita (log,sc)	3.168***(2.22, 4.70)
Democracy	0.817 (0.45, 1.50)
Constant	2.62 (0.09, 73.16)
Concordance	0.69

Note: Results are from the generalized linear model. There are 2,470 observations and 94 events. All variables but `Democracy` are standardized. All results are based on two-tailed tests. ^p<0.1; *p<0.05; **p<0.01; ***p<0.001

3.5 Alternative Model Specification

In addition to employing a CPH Model, we also use a Generalized Linear Model (GLM). As Model 1 in Table 5 shows, the results are robust to this alternative model specification.

References

Anselin, Luc. 2001. “Spatial econometrics.” *A companion to theoretical econometrics* 310330.

Beck, Nathaniel, Jonathan N Katz and Richard Tucker. 1998. “Taking time seriously: Time-series-cross-section analysis with a binary dependent variable.” *American Journal of Political Science* 42(4):1260–1288.

Beck, Nathaniel and Simon Jackman. 1998. “Beyond linearity by default: Generalized additive models.” *American Journal of Political Science* 42:596–627.

Betz, Timm, Scott J Cook and Florian M Hollenbach. 2019. “Bias from network misspecification under spatial dependence.” *Political Analysis* pp. 1–7.

Box-Steffensmeier, Janet M, Dan Reiter and Christopher Zorn. 2003. “Nonproportional hazards and event history analysis in international relations.” *Journal of Conflict Resolution* 47(1):33–53.

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

Fowler, James H and Nicholas A Christakis. 2010. “Cooperative behavior cascades in human social networks.” *Proceedings of the National Academy of Sciences* 107(12):5334–5338.

Grambsch, Patricia M and Terry M Therneau. 1994. “Proportional hazards tests and diagnostics based on weighted residuals.” *Biometrika* 81(3):515–526.

Juhl, Sebastian. 2020. “The sensitivity of spatial regression models to network misspecification.” *Political Analysis* 28(1):1–19.

Keele, Luke. 2010. “Proportionally difficult: testing for nonproportional hazards in Cox models.” *Political Analysis* 18(2):189–205.

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

Ruppert, David, Matt P Wand and Raymond J Carroll. 2003. *Semiparametric regression.* Number 12 New York: Cambridge University Press.

Shadden, Mark and Christopher Zorn. 2011. Data transformations for social science research: Theory and best practices. In *In annual meeting of Society for Political Methodology, Princeton, NJ, June.* pp. 28–30.

Shalizi, Cosma Rohilla and Andrew C Thomas. 2011. “Homophily and contagion are generically confounded in observational social network studies.” *Sociological methods & research* 40(2):211–239.

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.

Stinnett, Douglas M, Jaroslav Tir, Paul F Diehl, Philip Schafer and Charles Gochman. 2002. “The correlates of war (cow) project direct contiguity data, version 3.0.” *Conflict Management and Peace Science* 19(2):59–67.

Therneau, Terry, Cynthia Crowson and Elizabeth Atkinson. 2020. “Multi-state models and competing risks.” *CRAN-R (https://cran. r-project. org/web/packages/survival/vignettes/compete. pdf)* .

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

Therneau, Terry M, Patricia M Grambsch and Thomas R Fleming. 1990. “Martingale-based residuals for survival models.” *Biometrika* 77(1):147–160.