Online Appendix:
Data, Method, & Robustness Checks

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

Nadiya Kostyuk & Jen Sidorova

December 3, 2025

Contents

1 New Data on National Cybersecurity Strategies

We have compiled a highly comprehensive dataset of national cybersecurity strategies, titled the *National Cybersecurity Strategies* (NCS) dataset (v1.0). This dataset covers all national cybersecurity strategies adopted by states from 2020 to 2024. To ensure the relevance and reliability of the data, we primarily sourced the documents from official government websites. In line with best practices in conflict studies, we cross-referenced multiple sources to validate the inclusion of each strategy (Woolley, 2000). In particular, we consulted databases curated by international organizations such as the International Telecommunication Union (ITU), the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), and the United Nations Institute for Disarmament Research (UNIDIR). In cases where information was limited or ambiguous, we reached out to country-specific experts for clarification.

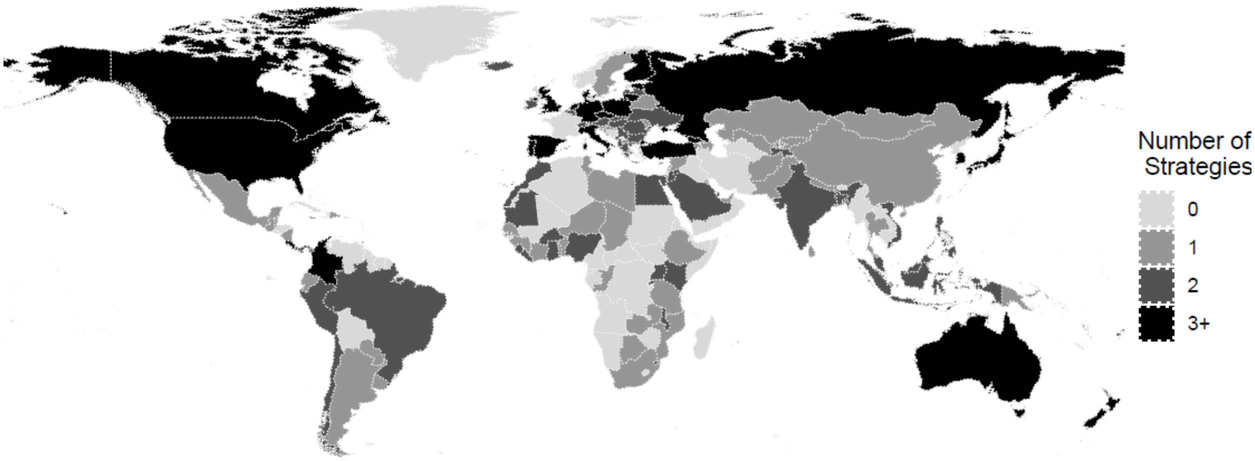
The NCS dataset includes 246 strategies from 135 countries. For countries where no strategy was found, we recorded that a national cybersecurity strategy has not yet been released. We plan to update the dataset on a regular basis (e.g., biannually) to incorporate newly published strategies and any revisions to existing ones.

The NCS dataset consists of two main components. First is **Structured Metadata Spreadsheet.** This Excel file records key information for each strategy, including the publication date, official title, and the governmental body responsible for its release, strategy length, language of publication (e.g., English, native language, or both). While strategies may be authored by different national entities (e.g., the White House, Ministry of Communication and Information Technology), we have ensured that the dataset includes only national-level cybersecurity strategies—those that outline a country's overarching cyber policy.

We excluded agency-specific strategies (e.g., a Ministry of Transportation's cybersecurity policy) and international strategies not directly tied to a single nation-state. National cybersecurity strategies are comprehensive documents that reflect a government's unified approach to managing cyber risks across sectors, whereas agency-specific strategies are limited in scope and designed to address cybersecurity within a specific domain or ministry. International strategies, meanwhile, typically have an outward-looking focus, emphasizing regional cooperation, global norms, and collaborative frameworks rather than domestic policy priorities. The next version of the NCS dataset will expand to include these other types of strategies, as well as broader digital policy documents (e.g., digital agendas, e-government strategies, etc.).

It is also worth noting that while some countries have published only a single strategy, many have released successive versions over time. The current version of the dataset records all such iterations. For a breakdown of how many strategies each country has published as of 2024, see Figure 1 below.

Figure 1: *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.

The research team used the following codebook and instructions to create the structured metadata spreadsheet.

1. **publication_date**: The date when a strategy was published, using the YYYYMMDD format. If only the publication year is available, use 'YYYY0101'. If only the year and month are available, use 'YYYYMM01'.
2. **country**: Publishing country.
3. **short_title**: Use 'Cybersecurity Strategy' for national cybersecurity strategies.
4. **official_title**: The official title of the document.
5. **revised_edition**: A dummy variable indicating whether a new strategy is a revised edition of the previously published strategy.
6. **publication_agency**: The governmental body responsible for releasing the strategy.
7. **strategy_number:** indicates the chronological order of the strategy published by the country (e.g., 1 = first strategy, 2 = second strategy, etc.).
8. **strategy_length**: Number of pages. Please include only a numeric value.
9. **pdf_available**: a dummy variable indicating whether a pdf of the strategy is available.
10. **txt_available**: a dummy variable indicating whether a txt of the strategy is available.
11. **marker_available**: a dummy variable indicating whether a txt of the strategy was processed using Marker AI. 0 identifies non-Marker files, created using this OCR technique.
12. **publication_language**: The language of publication (e.g., English, native language, or both).
13. **notes**: Any relevant notes.

Second is **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. In this case, Marker AI will perform the additional step of recognizing text before processing, which is very computationally expensive. For these cases, the text files (referred to as Non-Marker files) were created using an OCR (Optical Character Recognition) technique.[1] OCR converts scanned documents with images of text into machine-readable text by detecting the characters in the image and matching them with known characters. This alternative method extracted only the text, and no illustrations were retrieved.

There were also a few strategies where we were not able to find pdfs. Here is a list of such documents:

- 20230830_Azerbaijan_National Cybersecurity Strategy. As of 5/1/25, according to this link, the strategy was adopted, but we cannot find the text of the actual document.
- 20190801_Congo_National Cybersecurity Strategy. The document was published in French; the original link stopped working as of 04/26/25.
- 20160101_Fuji_National Cybersecurity Straetgy. Fiji adopted this cybersecurity strategy; unfortunately, no electronic version has been found, as mentioned by this source.
- 20220101_Namibia_National Cybersecurity Strategy (National Cybersecurity Strategy and Awareness Creation Plan 2022-2027): no electronic version publicly available, according to this source; cannot find an official document as of 4/26/25
- 20030101_Norway_National Cybersecurity Strategy. P. 3 of the 2019 Norwegian strategy says: "The present strategy is Norway's fourth cyber security strategy,"... "The first national Norwegian cyber security strategy was introduced in 2003; we were not able to find a pdf online (checked both English/Norwegian)
- 20210101_Peru_National Cybersecurity Strategy_ESP.pdf: this website lists that there was draft strategy published in Spanish as of 2021, however the document is not found as of 5/1/25.
- 20130101_Vanuatu_National Cybersecurity Strategy_FRN.pdf: according to this website, there was a strategy published in 2013; however, the referenced link is not available as of 4/26/25.
- 20160101_Vietnam_National Cybersecurity Strategy_ENG.pdf: according to this website, there was a strategy published in 2016; however, the referenced link is not available as of 4/26/25.

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

- 20211001_Georgia_National Cybersecurity Strategy_ENG.pdf: according to this link, the strategy was adopted; however, the provided link to the official website is not working as of 5/1/25.
- 20220407_Guinea_National Cybersecurity Strategy_FRN.pdf: No official website was found; but this link mentions that the strategy was released.

The full dataset, including the spreadsheet and all associated documents, are available on the following website: National Cybersecurity Strategies Data.

2 Summary Statistics

Figure 2 displays the correlation plot for the main explanatory variables. Table 1 shows the summary statistics for these variables and our outcome of interest.

Figure 2: Correlation Plot

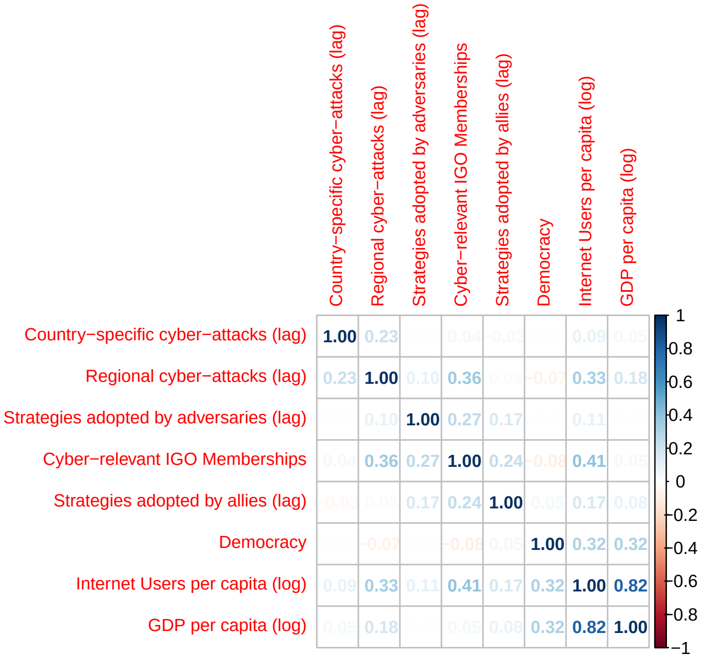


Table 1: *Summary Statistics*

	Minimum	*Median*	*Mean*	*Maximum*
Adoption	0.00	0.00	0.04	1.00
Country-Specific Cyber-Attacks (lag)	0.00	0.00	0.07	10.00
Regional Cyber-Attacks (lag)	0.00	0.00	5.30	38.00
Strategies Adopted by Adversaries (lag)	0.00	0.00	0.02	1.00
Cyber-relevant IGO Memberships	3.00	33.00	41.10	117.00
Strategies Adopted by Allies (lag)	0.00	0.00	0.02	1.00
Democracy	0.00	1.00	0.51	1.00
Internet Users per capita (log)	0.00	2.61	2.47	4.60
GDP per capita (log)	4.73	7.92	7.97	11.65

3 Empirical Strategy

3.1 Spatial lags

To identify the effect of the strategies adopted by a country's allies and adversaries, 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 allies/adversaries in $t-1$. Each element in $W_{i,-i}$ measures whether countries signed a military alliance treaty or whether they are adversaries. $\sum_{i=1,\ldots,N} W_{i,-i}$ 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 ally, then this relationship has a weight of 100%; consequently, the ally will most likely have a significant influence on this country's foreign policy decisions. On the other hand, if a nation has twenty allies and each relationship has a weight of 5%, then the influence of an individual ally on the country's foreign policy decisions will most likely be limited. $y_{-i}([t-1])$ represents whether a country's ally/adversary $-i$ 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 allies/adversaries that adopted or did not adopt cybersecurity strategies in $t-1$.

3.2 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:

$$\begin{aligned}\log(H(T_i)) \propto\ & \beta_1 \text{Country-Specific Cyber-Attacks}_i(\lfloor T-1 \rfloor, \lfloor T \rfloor) \\ & + \beta_2 \text{Cyber-Relevant IGO Membership}_i(\lfloor T \rfloor) \\ & + \beta_3 \text{Strategies Adopted by Allies}_i(\lfloor T-1 \rfloor, \lfloor T \rfloor) \\ & + \beta_4 X_i(\lfloor T \rfloor),\end{aligned}$$

where: $log(H(T_i))$ is the log of a hazard ratio that stands for the relative risk of country i adopting a cybersecurity strategy at time T; Country-Specific Cyber-Attacks$_i(\lfloor T-1 \rfloor, \lfloor T \rfloor)$ includes a number of cyber-attacks that a country experienced in a prior year; Cyber-Relevant IGO Memberships$_i(\lfloor T \rfloor)$ includes a cumulative number of IGOs where cybersecurity have been discussed as of the previous year;[2] Strategies Adopted by Allies$_i(\lfloor T-1 \rfloor, \lfloor T \rfloor)$ is the effect of inaugural national cybersecurity strategies adopted by allies in the previous year; $X_i(\lfloor T \rfloor)$ is a matrix of k exogenous variables; and β_4 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 number of the country's Internet users as a percentage of its total population in a given year (`Internet Users per Capita`); and[3] (3) a factor variable indicating the region to which each country belongs, based on World Bank classifications. Africa is used as the baseline category in the analysis.

4 IGOs Included in the Study

This section presents a list of intergovernmental organizations (IGOs) included in the analysis. Table 2 details the years when specific IGOs began addressing cybersecurity, while The full list of IGOs was sourced from Pevehouse et al. (2019)'s dataset, which records each country's membership in IGOs by year.

Table 2: The Onset of Cybersecurity Focus Among Intergovernmental Organizations

Organization	Year	Description	Source
AACB	2019	Approved dispatching FinTech and cybersecurity activities across CABS working groups; and tabled the Draft Report of the Experiences and Initiatives of AACB Member Central Banks in FinTech and Cyber Security at the 42nd Assembly.	Link

Continued on next page

[2] Section 4 includes a full list of these IGOs and years when they added cybersecurity to their agenda.

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

Table 2 – continued from previous page

Organization	Year	Description	Source
AALCO	2014	Formal "International Law in Cyberspace" agenda item. Introduced at the 53rd Annual Session (Tehran); since then it's been on AALCO's agenda with studies and OEWG meetings.	Link
AATA	2017	ATAF's June 2017 newsletter on the African Tax Outlook process recommended to "Implement data protection and information security of countries' data."	Link
ABEDA	2018	BADEA notes it obtained ISO 27001 (Information Systems Security) alongside ISO 9001 and ISO 20000 (shown on BADEA's official timeline).	Link
ACML	2024	ACMLS's 2024 book "Artificial Intelligence in Healthcare" explicitly discusses risks to patient safety and ...(cybersecurity).	Link
ACS	2021	An ACS press release for a March 23 & 31, 2021 maritime course (with DP World) lists "maritime cybersecurity" among the capacity-building topics.	Link
ACU	2016	The 45th ACU Board (Myanmar, 2016) decided on the importance of cybersecurity for payment and settlement systems; this was explicitly deliberated again at the 46th Board in Colombo (July 14, 2017) per the Central Bank of Sri Lanka's notice and press release.	Link
AFESD	2020	AFESD-coauthored Joint Arab Economic Report (JAER) 2020 discusses national cybersecurity strategies within Arab digital-economy policy.	Link
AFPU	2018	PAPU's 37th Administrative Council (Algiers, Apr 2018) ran a "Global Digital Postal Agenda" workshop whose Dot Post session covered "strategic digital initiatives, cyber security, e-commerce and standards."	Link
AfricaRice	2014	AfricaRice adopted an Open Access and Data Management Policy, effective May 1, 2014, committing to protect information products, ensure safe server storage/backup, and respect privacy of personal data—i.e., concrete information-security measures.	Link
AFRISTAT	2012	Terms of reference for an IHPC software workshop include procedures for securing databases, server security, and handling virus attacks/antivirus/firewall—clear cyber-security practices.	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
AFSPC	2018	PFTAC's official minutes report that, as follow-up to the 2018 AFSPC meeting, a "Cyber and IT Risk workshop [was] held in August 2018," which identified gaps and led to work on cybersecurity/IT-risk prudential standards, supervisory guidance, and an on-site examination framework.	Link
AGPUNDO	2009	AOU introduced an MSc in Computing (Cyber Security & Forensics) that was first validated in 2009. AOU has since expanded cyber programmes (e.g., BSc Cyber Security).	Link
AIC	2022	Formalizes cybersecurity governance by setting up a specialized and independent function to manage cyber risks, including defining frameworks and appointing an Information Security Officer.	Link
AIDO	2019	AIDMO co-organized a 2019 expert meeting on AI & local industrial development; conclusions reference privacy, cybersecurity, and corporate security.	Link
ALO	2018	ALO's Morocco workshop page for the Arab Labor Market Information Network states the platform applies standards for information security and cybersecurity.	Link
ALSF	2022	ALSF Academy's Oil & Gas Level 2 handbook states that cybersecurity is an increasingly necessary part of the security risk assessment.	Link
AmCC	2024	ACTO's IT Systems Specialist posting explicitly requires cybersecurity expertise, showing cyber-risk is addressed in infrastructure.	Link
AMF	2018	The Arab Regional Fintech Working Group includes "cyber risks" in its mandate; agenda includes data privacy.	Link
AMIPO	2022	In 2022, OAPI issued a tender to implement a security system for its computer network.	Link
AMU	2012	UMA co-organized a Rabat workshop on harmonizing cyber-legislation around essential infrastructure, e-government, and anti-cybercrime.	Link
Andean	2022	ADA's 2022 "Hoja de Ruta" calls for policies on cybersecurity and creating a trust network among national digital-security teams.	Link
ANZUS	2011	At AUSMIN 2011, Australia and the U.S. endorsed a joint statement on cyberspace; ANZUS was said to apply to cyberspace.	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
AOAD	2023	AOAD confirmed involvement in Arab Coordination Committee meetings focusing on digital economy and cybersecurity.	Link
APEC	2002	The APEC Cybersecurity Strategy issued in 2002 outlined cybercrime legislation, technical standards, and training initiatives.	Link
APIBD	2020	AIBD organized a webinar on "Managing Cybersecurity during COVID-19" for 30 countries.	Link
APO	2010	APO's first e-learning course on Information Security Management Systems held in 2010; followed by ISO/IEC-based courses.	Link
APT	2009	APT filed WTDC-10 proposals on cooperation for cybersecurity and established PacCERT for the Pacific.	Link
ARC	2025	ARC's 2025 Whistleblower Policy flags cyber-type misconduct as reportable violations (e.g., unauthorized access, data theft).	Link
ARIPO	2023	ARIPO issued an RFP for IT Security Audit Services; a 3-year cybersecurity strategy was recommended.	Link
ARPU	2024	The 45th Arab Permanent Postal Committee (APPC) listed "Cybersecurity" among the meeting themes.	Link
ArticC	2016	Arctic Council reported efforts to enhance cybersecurity and adopt secure platforms for collaboration.	Link
AsDB	2016	ADB's 2016 paper on smart grids includes a dedicated section on "Cyber Security Issues for the Bulk Power System."	Link
ASEAN	2012	ASEAN Regional Forum adopted its first cyber cooperation statement in Phnom Penh in July 2012.	Link
ASECNA	2017	ASECNA participated in the "Assessment of AFI Aeronautical Networks Cyber Security" initiative.	Link
ASEF	2017	ASEF's Outlook Report 2016/2017 includes a section "Cybersecurity," showing the topic is addressed in official publications.	Link
AU	2014	AU Heads of State adopted the African Union Convention on Cyber Security and Personal Data Protection (the "Malabo Convention") on 27 June 2014 — the AU's foundational cyber & data-protection instrument (entered into force June 2023).	Link
BC	2007	The 13th Baltic Council Joint Statement (23 Nov 2007) lists as 2008 priorities: "Cooperation in fighting cyber crime; security of the cyber-space."	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
BENELUX	2015	A Benelux General Secretariat newsletter (Nov 2015) set cybersecurity as a priority, noting national strategies, creation of Cyber Security Boards/CERTs, and operational collaboration between the three government CERTs	Link
BIPM	2016	CIPM 2016 minutes note BIPM's commitment to bring cybersecurity to the highest standard (with external IT audit).	Link
BIS	2016	CPMI–IOSCO Guidance on cyber resilience for FMIs (29 Jun 2016) – the globally agreed cyber-resilience guidance for payment, clearing and settlement infrastructures.	Link
BOBP	2023	The organization has discussed "Cyber Security" in its event materials (as part of technology and security themes highlighted in BOBP-IGO sessions, 2023).	Link
BORGIP	2020	BOIP obtained ISO/IEC 27001 information-security certification (certificate May 2020; news 8 Jul 2020).	Link
CAIPA	2020	ICAP published guidance on "Ciber-COVID19: efectos y retos para Centroamérica" (19 May 2020) and "La importancia de la ciberseguridad" (Spanish/English posts), explicitly addressing cyber risks for public institutions.	Link
CBSS	2020	In Oct 2020, CBSS ran an EUSBSR Forum workshop on "Risks and (untapped) potential of digitalisation in ports and at sea," explicitly flagging the "rising threat of cyberattacks" and recommending stakeholders "strengthen their monitoring systems and upgrade outdated ones."	Link
CDB	2017	CDB's Office of Integrity, Compliance & Accountability says it "paid special attention to the threat of cybercrime," issued staff advisories on ransomware, and hosted mandatory cybersecurity/cybercrime training in July 2017 with the FBI.	Link
CEI	2017	CEI was a partner in SECNET (Interreg Italy–Slovenia) to enhance port security with pilot actions focused on cyber-security; project kick-off 2017 and activities ran 10/2017–03/2019.	Link
CEMAC	2022	COBAC later alerted institutions to strengthen cybersecurity/IT-risk controls via circular LC-COB/04 of 21 Jan 2022 (widely referenced by regional compliance notes and press).	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
CERN	2000	CERN's binding Computing Rules (Operational Circular No. 5) date to October 2000 (revised 2022/2024), establishing the organisation's formal computer-security regime.	Link
CIS	2001	CIS member states signed the Agreement on Cooperation in Combating Offences related to Computer Information on June 1, 2001	Link
COE	2001	The Convention on Cybercrime (Budapest Convention) was then opened for signature on 23 Nov 2001 (ETS 185).	Link
COLOMBO	2018	The 46th Consultative Committee Meeting Report (2018) lists "cyber security" among priority issues considered by members.	Link
COMESA	2012	The Council of Ministers (2012)urged Member States to domesticate the COMESA model policy, law and regulations on cyber security.	Link
ComSec	2011	Law Ministers mandated a cybercrime experts' working group in July 2011, leading to the Commonwealth Cybercrime Initiative (CCI); Heads later endorsed the Commonwealth Cyber Declaration (2018).	Link
CSTO	2006	The CSTO itself says that "the formation of an information-security system ... began in 2006."	Link
D8	2021	First D-8 Senior Experts Meeting on ICT (8 Sept 2021): delegates "emphasized ... 5G technologies and Cyber Security" as priority cooperation areas.	Link
EAC	2015	The EAC Model ICT Policy Framework (2015) encourages member states to establish mechanisms for regional and international cooperation on cybersecurity	Link
EAEC	2011	The Customs Union Commission Decision No. 771 (16 Aug 2011)—adopted under EurAsEC's Customs Union—sets the technical policy for the Integrated Information System and requires that "information security" be ensured (with unified requirements) when building and interconnecting national systems.	Link
EAPC	2008	EAPC seminar on cyber defence held in Yerevan, 23–25 June 2008	Link
EBRD	2009	Policy on the Use of Bank IT Facilities (2009) sets specific security requirements (e.g., password rules), and later strategy papers commit to improving our cyber security and launch client-facing cyber programmes (e.g., Cybersecurity Resilience Programme, 2023).	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
ECB	2017	Eurosystem adopted a Cyber Resilience Strategy for FMIs in 2017 and the ECB published the Cyber Resilience Oversight Expectations (CROE) in December 2018.	Link
ECCA	2016	The ECCB's 2015/2016 Annual Report records "Information Security audits focusing on high-risk IT systems."	Link
ECCAS	2011	Under the ITU–EU HIPSSA programme, ECCAS prepared model laws on personal data protection, electronic transactions, and cybercrime control; these were validated at ECCAS regional workshops in Libreville (28 Nov–2 Dec 2011) and Douala (16–18 Jul 2012) with the ECCAS Secretariat's participation.	Link
ECO	2006	the first ECO Interior Ministers' meeting launched work on a regional plan against transnational organized crime including "cyber crimes." The subsequent Plan of Action (drafted 2010) calls on Member States to share information and best practices on Cyber Crimes	Link
ECOWAS	2011	ECOWAS adopted Directive C/DIR/1/08/11 on Fighting Cybercrime within ECOWAS (Council of Ministers, 19 Aug 2011). The directive adapts Member States' substantive and procedural criminal law to cybercrime.	Link
EFTA	2005	EFTA (via the EEA pillar for Iceland, Liechtenstein, Norway) incorporated the EU law that created ENISA (the EU cybersecurity agency) into the EEA Agreement.	Link
EIB	2015	In its 2015 Annual Report on operations inside the EU, the EIB explicitly broadened tech lending to cover "software, automation and cyber security."	Link
EIPA	2015	EIPA's EPSA publication (2015) profiles The Hague Security Delta and its Cyber Security Academy, showing EIPA was already discussing cybersecurity policy and ecosystems by 2015.	Link
EMI	2000	EMI/ECB's Report on electronic money (1997–1998) set "Requirement 3: Technical security" for e-money schemes to maintain safeguards that prevent, contain and detect security threats (including counterfeits).	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
ESA	2005	ESA's 2005 Annual Report says information security was "thoroughly reviewed" and that the latest ESA Security Regulations were adopted by Member States in 2005 (establishing the framework for handling classified information and IT security).	Link
EU	2001	The European Commission published COM(2001)298 ("Network and Information Security: Proposal for a European Policy Approach") on 6 June 2001, kicking off an EU-level NIS policy. The Council followed with a Resolution on a common approach and specific actions in the area of network and information security (28 Jan 2002)	Link
EURATOM	2001	The Commission adopted Decision 2001/844/EC, ECSC, Euratom (29 Nov 2001), laying down security rules for EU classified information (EUCI) that apply across the Commission and bodies operating under the **EC/ECSC**/Euratom treaties. The annex includes rules for information-technology and communications systems handling EUCI—an explicit, dated information-security framework covering Euratom activities.	
G24	2018	At the G-24/AFI roundtable, AFI's special report for the event explicitly listed "cybersecurity" among the policy/training priorities for digital financial inclusion (Sept 2018).	Link
GCC	2022	The GCC Ministerial Committee for Cybersecurity held its first meeting on Oct 23, 2022 at the GCC Secretariat in Riyadh; the archive also notes the first GCC cybersecurity exercise in 2022.	Link
IAEA	2011	IAEA issued Nuclear Security Series No. 17, Computer Security at Nuclear Facilities (2011), the first Agency-wide technical guidance integrating computer/cyber security into nuclear security programmes.	Link
IAIC	2016	The IDB Group (of which IIC/IDB Invest is the private-sector arm) announced a cybersecurity partnership with the Government of Israel to fund capacity building in Latin America and the Caribbean.	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
IAIGC	2020	IAIGC/Dhaman's flagship Investment Climate in Arab Countries report explicitly evaluates "crime & security … including cyber crime," i.e., it began discussing cyber risk in its assessments at least in the 2020 edition.	Link
IBEC	2017	IBEC publicly engaged on "bank information security issues" as a silver sponsor of the 34th BACEE Regional Banking Conference (Budapest), 12 Apr 2017.	Link
IBRD	2016	The Bank launched the Global Cybersecurity Capacity Program (2016–2019) to help countries assess maturity and build capacity (CMM reviews, TA, workshops). This is the first formal, Bank-run cyber capacity program we can document.	Link
ICC	2008	By 2008 the ICC had created an Information Security Management Forum (ISMF) (ICC/INF/2008/003), cited in Assembly of States Parties records.	Link
IEA	2012	The IEA-affiliated Technology Collaboration Programme ISGAN published Smart Grid Cyber Security (white paper), explicitly framing smart-grid cyber risk and policy needs.	Link
IFC	2016	IFC's Corporate Governance paper (April 2016) flags cyber security as a top issue for companies (statement by an IFC Corporate Governance Officer).	Link
IMF	2011	The IMF publicly acknowledged and addressed a cyber incident in June 2011 during an official press briefing ("update on the cyber incident at the Fund… we're still investigating this breach").	Link
IMO	2017	The Maritime Safety Committee adopted Resolution MSC.428(98) (16 June 2017) on Maritime Cyber Risk Management (to be integrated into ISM safety management systems).	Link
INTERPOL	2000	The General Assembly (Beijing, 4–10 Oct 1995) adopted Resolution AGN/64/RES/22 "Computer-related crime," calling for regional initiatives, a small expert steering committee, standardized methods for international computer investigations, and rapid information exchange—INTERPOL's earliest formal, global mandate on cybercrime.	Link
IOCom	2013	That same 2013 IOC conference materials flagged cybersecurity problems and cross-border impacts (e.g., phishing)—the earliest explicit IOC reference to cyber issues I could find.	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
IRENA	2019	IRENA devoted a subsection “Cybersecurity” in its 2019 geopolitics report, discussing digitalization risks to grids and calling for common cybersecurity norms.	Link
ISDB	2018	IsDB reported approval of its Information Security Policies by Senior Management in 2018, and launched an internal digitalization program (“MyIsDB” app, mail digitization).	Link
ITU	2007	ITU launched the Global Cybersecurity Agenda (GCA) as a cooperation framework for cybersecurity.	Link
LAEO	2024	In June/July 2024 OLADE published an editorial and newsletter making cybersecurity an urgent priority for the region’s energy sector; OLADE also produced a talk on “La ciberseguridad y su rol en el sector energético.”	Link
LAIA	2022	ALADI’s Secretariat published a regional diagnostic on the digital economy that explicitly assesses member states’ “ciberseguridad” capabilities (incident-response entities, etc.).	Link
LAIEC	2017	ILCE’s Red Escolar ran the collaborative project “Escuadrón Ciberespacio” in 2017, aligned with Mexico’s Federal Police “Campaña Ciberseguridad 2017.” That’s the earliest explicit ILCE-branded cyber effort I can verify.	Link
LOAS	2010	The Arab Convention on Combating Information Technology Offences was adopted on 21 Dec 2010 in Cairo under the League of Arab States (signed by Arab interior and justice ministers; deposited with the LAS General Secretariat).	Link
Mercosur	2014	The Council of the Common Market created the “Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica (RAPRISIT)”, explicitly citing the need to address “seguridad cibernética”. CMC/DEC No. 17/14, Caracas, 28 Jul 2014.	Link
MIGA	2007	MIGA’s 2007 Annual Report says “for data security, more robust reporting functions and security monitoring have been implemented to further enhance MIGA’s information security,” showing an explicit information-security program by 2007. Later MD&A filings describe a formal cybersecurity risk-management program (e.g., FY20–FY24).	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
NAM	2013	In the UN First Committee, Indonesia on behalf of NAM stated: "information and communication technologies have the potential to endanger international peace and security," calling for a UN legal framework — a clear NAM position on cybersecurity/ICT security. (7 Oct 2013).	Link
NATO	2002	Cyber became a NATO political agenda item at the Prague Summit, launching a Cyber Defence Programme; this led to the NATO Computer Incident Response Capability (NCIRC) (first "cyber first-responder" capacity).	Link
NCM	2004	NCM formally adopted the Northern e-Dimension Action Plan (NeDAP) in Aug 2004, which includes Action Line 2: "A Secure Information Infrastructure".	Link
NIB	2014	NIB's Annual Review 2014 describes operational risk controls including "security arrangements to protect the physical and ICT infrastructure of the Bank"—an explicit information-security remit.	Link
NordC	2013	The Nordic Council's Theme Session 2013 agenda explicitly included a "Member's proposal on strengthening Nordic co-operation in security and defence policies against cyber threats and digital attacks (A 1581/Presidium)".	Link
OAPEC	2021	OAPEC's Technical Affairs Department published a study on digital transformation in refining/petrochemicals that explicitly defines and discusses "Cyber security".	Link
OAS	2000	OAS Ministers of Justice (REMJA) created a Working Group on Cyber-crime and held its first meeting on May 12, 1999 (agenda and final report describe the 1999 experts' meetings and mandate).	Link
OECD	2000	OECD Council adopted the "Guidelines for the Security of Information Systems" on 26 Nov 1992 (first intergovernmental cyber/infosec guidance at the OECD).	Link
OECS	2019	OECS press release highlights ARIN's 2019 Caribbean outreach "focusing on cyber security and Internet resilience."	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
OIC	2008	The OIC created the OIC-CERT (OIC Computer Emergency Response Team). The 35th Council of Foreign Ministers first adopted a resolution to collaborate among national CERTs in June 2008, and the 36th CFM granted OIC-CERT affiliated-institution status in May 2009; OIC-CERT has operated since 2009.	Link
OPEC	2020	OPEC's Second Workshop on Energy & Information Technology (21 Sep 2020) explicitly focused on topics including "cyber security" for the oil sector.	Link
OSCE	2004	Earliest OSCE ministerial decision on a cyber issue targeted terrorist misuse of the Internet (MC.DEC/3/04, 7 Dec 2004).	Link
OSPAR	2021	OSPAR Secretariat objectives for 2021–2023 include maintaining security of the OSPAR Secretariat IT system (an information-security/cybersecurity function).	Link
PAHO	2016	PAHO reports it received strategic advisory services on cybersecurity in 2016 from the UN International Computing Centre and defined a Cybersecurity Roadmap.	Link
PAP	2018	PAP adopted a Recommendation on the ICT sector that explicitly urges states to "sign, ratify and domesticate the African Union Convention on Cyber Security and Personal Data Protection," and to establish national CERT/CSIRTs and cyber-crime reporting mechanisms.	Link
PIF	2018	Forum Leaders adopted the Boe Declaration on Regional Security on 5 Sept 2018, which explicitly expands regional security to include cybersecurity / cyber-enabled threats. The Forum's page and summaries confirm this scope; the Boe Declaration Action Plan (2019) implements it.	Link
RCC	2011	RCC's Annual Report 2010–2011 lists work on "countering terrorism, cyber security and defence procurement," i.e., the RCC was already treating cybersecurity as a program area by that time.	Link
RCFC	2003	RCC set up a dedicated Working Group on Information Security of Interoperable Communication Networks under its Operators Board, created by Decision No. 13/5 of 30 Oct 2003.	Link
SAARC	2014	SAARC Leaders at the 18th Summit (Kathmandu, 27 Nov 2014) "agreed to establish a cyber crime monitoring desk."	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
SADC	2012	SADC adopted a harmonised cybersecurity legal & regulatory framework built around three SADC Model Laws — Computer Crime & Cybercrime, Data Protection, and Electronic Transactions & E-Commerce — approved by SADC ICT/Telecom Ministers in 2012.	Link
SCHENGEN	2000	The 1990 Convention implementing the Schengen Agreement (CISA) hard-codes IT-security controls for the Schengen Information System (SIS) — e.g., Article 118 requires equipment access control, data-media control, user control, audit of inputs/transfers, and secure communications; it also ties processing to the Council of Europe data-protection instruments.	Link
SCO	2006	SCO Heads of State adopted the "Statement on International Information Security," launching a dedicated IIS/cyber track.	Link
SEGIB	2012	The 1st Ibero-American Meeting of Interior and Public Security Ministers (Valencia, 17–18 Sept 2012) — convened in the SEGIB framework for the XXII Summit — explicitly lists "delito cibernético" (cybercrime) among the priority crimes for joint action and proposes creating an IT training network between national police academies.	Link
SELA	2015	SELA co-organized a distance course on the legal aspects of e-commerce for the Caribbean (23 Mar–19 Apr 2015) whose syllabus explicitly includes "Seguridad en el Comercio Electrónico" and "Privacidad en línea."	Link
SICA	2009	A SICA-hosted agenda in 2009 included a session on "delitos telemáticos e informáticos" (telematic & computer crimes) — an early, explicit SICA treatment of cyber-crime.	Link
SPC	2010	SPC prepared and coordinated the Framework for Action on ICT for Development in the Pacific (FAIDP) (prepared at SPC Suva, 2010), which includes Theme 6: "Cyber security and ICT applications," with 2011–2015 strategies such as supporting PacCERT and encouraging national CERTs.	Link
SWPD	2019	At the 17th SwPD Ministerial (Bangkok, 1 Aug 2019), ministers listed "inter-connectivity and cyber security" among the meeting's focus areas.	Link
UEMOA	2013	WAEMU's Common Policy on Peace & Security (adopted 24 Oct 2013) lists fighting "la cybercriminalité" among its objectives.	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
UM	2016	The UfM's Digital Economy & Internet Access Working Group (DEWoG) workplan for 2016 included a work item on "Ensuring cybersecurity" (with CVE linkage).	Link
UN	2000	The UN General Assembly adopted resolution 53/70 on "Developments in the field of information and telecommunications in the context of international security," launching the UN's cybersecurity/IIS track.	Link
UNESCO	2000	INFOethics 2000 materials explicitly call for protecting "security and privacy ... through ... encryption," and for governments to guarantee citizens' security and privacy online.	Link
UNIDO	2004	In its "High-Tech Regional Programme to Increase Industrial e-Productivity" UNIDO ran training on "information safety management" covering ISO 17799 and BS 7799-2 (information-security management systems) on 24–25 Nov 2004.	Link
UPU	2003	The UPU adopted Standard S43 (Secure Electronic Postal Services / Electronic PostMark interface) in 2003, i.e., a cybersecurity/trust framework for e-postal services.	Link
VASAB	2023	VASAB's Vision 2040 text explicitly flags "cyber resilience and cyber security issues" and calls for cooperation to address cyber threats across the Baltic Sea Region (draft 2022; final 2023).	Link
WAHO	2023	WAHO's procurement templates were updated to include provisions to manage cybersecurity risks; a 2025 WAHO Request for Proposals quotes the July 2023 revision and shows the specific "cybersécurité" clauses bidders must address.	Link
WCDC	2018	Under ARGE patronage, the conference "Digitalization in the Danube Region" (24 May 2018) explicitly discussed e-government and cyber-security—showing ARGE addressing the topic by 2018.	Link
WCO	2004	WCO deployed CENcomm, its secure global communication tool, to exchange operational intelligence; WCO material notes CEN became operational in 2000 and CENcomm followed in 2004.	Link
WHO	2018	The Digital health resolution (WHA71.7, 2018) tells countries to develop data-security and privacy policies for digital health.	Link

Continued on next page

Table 2 – continued from previous page

Organization	Year	Description	Source
WIPO	2002	WIPO formally documented an "Overview of WIPO's Information Security Policies" to the Standing Committee on Information Technologies (SCIT) on April 26, 2002. Follow-up governance documents for 2002–2003 record specific IT security policies (e.g., an Information Security Acceptable Use Policy).	Link
WMO	2006	A 2006 WIS brief notes the pilot explicitly considered encryption, authorization, privilege levels and authentication to ensure security of data—i.e., core cybersecurity controls.	Link
WTO	2017	WTO Members debated cybersecurity regulations in the TBT Committee on 15 June 2017 — e.g., concerns over China's draft encryption rules and cyber reviews.	Link
WTOURO	2012	UNWTO's internal ICT report explicitly says the Organization must "ensure cyber security standards," noting risks from social networks and the need for regular ICT reviews.	Link

5 Robustness Checks & Additional Results

We conduct the following robustness checks:

1. trends among alliances (Section 5.1);
2. alternative cyber-threat-environment measurement (Section 5.2); and
3. alternative model specification (Section 5.3);
4. accounting for regional biases in cyber-threat reporting; and
5. alternative measure of the influence of international organizations (Section 5.5.

5.1 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. To further explore the significance of a country's membership in different military alliances, we conducted an additional test to specifically account for the country's membership in the North Atlantic Treaty Organization (NATO). Model 1 in Table 3 shows that while membership in specific alliances, such as NATO, may have some influence, the strategies adopted by a country's allies play an important—and potentially even greater—role in the diffusion process.

5.2 Alternative Cyber-threat-environment Measurement

To measure perceived cyber threats and account for interstate competition as a driver of strategy adoption, we consider not only the actual cyber incidents a country has experienced, but also the

Table 3: Robustness Checks

	Model 1	*Model 2*	*Model 3*
	Allies	*Threats*	*Specification*
Strategies adopted by allies (lag,sc)	1.14*(1.02; 1.27)	——	0.21
Strategies adopted by adversaries (lag,sc)	——	1.05(0.95; 1.17)	——
Country-specific cyber-attacks (lag,sc) (DCID)	——	——	0.13
Cyber-Relevant IGO Memberships (lag, sc)	——	——	0.38
NATO Member	2.71***(1.55; 4.73)	——	——
Internet Users per Capita (log,sc)	3.02***(1.79; 5.09)	3.2***(1.9; 5.36)	0.83
Democracy	1.96**(1.22; 3.15)	2.04**(1.29; 3.24)	0.70
Asia	1.12(0.58; 2.15)	1.07(0.56; 2.05)	0.18
Europe	0.56(0.26; 1.22)	1.07(0.52; 2.21)	0.19
North America	0.67(0.3; 1.46)	0.69(0.31; 1.51)	-0.22
Oceania	1.81(0.64; 5.11)	1.71(0.6; 4.85)	0.41
South America	0.39^(0.15; 1.03)	0.38*(0.15; 0.99)	-0.71
Concordance (C-statistic)	0.75	0.74	0.87

Note: Models 1 and 2 use Cox Proportional-Hazards models, while Model 3 is a generalized linear model estimated with ridge regression. In Models 1 and 2, hazard ratios (exponentiated coefficients) above 1 indicate a positive association with strategy adoption, and values below 1 indicate a negative association. For Model 3, the reported coefficients are on the log-odds scale and have not been exponentiated. There are 2,649 observations and 107 events. All results are based on two-tailed tests. `log`: logarithmized; `sc`: standardized; `lag`: lagged. $^{\wedge}p<0.1$; $^{*}p<0.05$; $^{**}p<0.01$; $^{***}p<0.001$

possibility that cybersecurity strategies diffuse in response to adversaries' strategy adoption. This reflects the notion that the development of cybersecurity strategies by adversaries may serve as an indirect proxy for the development of cyber capabilities. To capture this dynamic, we record a weighted average effect of the cybersecurity strategies adopted by a country's adversaries prior to the adoption of its own first national strategy (`Strategies Adopted by Adversaries`).

Since states can attack one another using cyber and/or conventional means, we identify adversaries using Diehl, Goertz and Gallegos (2021)'s Peace Data (v3.01)[4] and DCID (v2.0). We use the NSC dataset to record when each identified adversary adopted its first national cybersecurity strategy. To represent the influence of adversarial diffusion without overcomplicating the model with numerous time-lagged variables, we follow the approach of Simmons and Elkins (2004). Specifically, we apply lagged network-weighted effects, which capture the average influence of a country's adversaries based on their relative significance. For example, if a country has only one adversary, that adversary is assigned a weight of 100%, indicating strong influence. Conversely, if a country has twenty adversaries, each is weighted at 5%, implying more diffuse influence.[5]

Model 2 in Table 3 demonstrates that the earlier obtained results hold—perceived threats are unlikely to contribute to the strategy diffusion.

[4] This data covers rivalries that have active war plans, frequent militarized disputes, absent communication, and no diplomatic recognition or diplomatic hostility.

[5] Additional details on the calculation of this weighted-average effect are provided in Online Appendix Section 3.1.

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

	Threats			
	Model 1	*Model 2*	*Model 3*	*Model 4*
Country-specific cyber-attacks (lag,sc) (DCID)	1(0.85; 1.18)	——	——	——
Country-specific cyber-attacks (lag,sc) (ERC)	——	1.17(0.64; 2.15)	——	——
Regional Cyber-attacks (lag,sc) (DCID)	——	——	0.49(0.18; 1.32)	——
Regional Cyber-attacks (lag,sc) (ERC)	——	——	——	0.72(0.19; 2.71)
Internet Users (log,sc)	7.32**(2.09; 25.58)	7.06**(1.95; 25.5)	6.02**(1.7; 21.33)	7.83**(1.89; 32.46)
Europe	0.87(0.11; 6.85)	1.24(0.15; 10.15)	0.19(0.02; 1.63)	0.78(0.19; 3.18)
North America	4.3(0.43; 43.52)	6.76(0.47; 96.83)	1.6(0.29; 8.65)	2.55(0.2; 31.79)
Oceania	2.83(0.28; 28.24)	4.64(0.29; 75.42)	0.51(0.03; 8.07)	1.69(0.13; 22.4)
South America	0.95(0.1; 8.89)	1.72(0.1; 29.02)	0.09(0; 2.18)	0.42(0.02; 10.16)
Concordance	0.74	0.74	0.76	0.75

Note: 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. $^{\wedge}$p<0.1; *p<0.05; **p<0.01; ***p<0.001

5.3 Alternative Model Specification

In addition to employing a CPH Model, we also use a Generalized Linear Model (GLM) estimated with ridge regression. As Model 3 in Table 3 shows, the results are robust to this alternative model specification.

5.4 Regional Biases of Cyber-threat Reporting

Under-reporting—particularly in regions outside North America and Europe—can introduce bias into cyber incident-level data. Even the primarily aim of the research note is to introduce the new data and not to comprehensively discuss the quality of cyber-incident dataset, it is important to acknowledge this data limitation. To assess whether our findings are sensitive to potential under-reporting, we re-run our models with cyber-threats using only data from regions with higher reporting confidence—specifically OECD countries.

Models in Table 4 present the robustness check results. Models 3 and 4, which include regional cyber-threats, confirm that such threats are unlikely to contribute to diffusion. Models 1 and 2, which assess actual (country-specific) cyber-threats, show that the direction of the effect remains positive, in line with the hypothesized relationship. However, the effect in Models 1 and 2 becomes statistically non-significant—likely due to reduced sample size and statistical power. Overall, this sensitivity analysis increases confidence that the observed effect is not solely driven by underreporting, though caution is still warranted given variation in data completeness and model sensitivity.

5.5 Alternative Measure of the Influence of International Organizations

Given the strong upward trend in `Cyber-Relevant IGOs Memberships` over time, we assessed its potential collinearity with time. To isolate the IGO effect from time trends, we regressed the IGO variable on a spline-transformed year term and saved the residuals, which we used as the main predictor in subsequent model. However, even after removing the time trend through residualization, multicollinearity persisted, and standard estimation produced inflated coefficient estimates. This was likely due to the tight correlation between increasing IGO memberships and time, alongside quasi-complete separation from the outcome.[6] To address this, we applied ridge regression in our model, which shrinks overly influential coefficients toward zero and improves model stability. Ridge regression is particularly appropriate in cases of multicollinearity or separation, as it reduces variance inflation without excluding variables from the model. Despite this more conservative estimation approach, the coefficient for `Cyber-Relevant IGO memberships` remained positive and statistically significant, with a notably large effect size (HR: 6.93; CI: 0.83–57.67). While the wide confidence intervals reflect uncertainty due to remaining collinearity, the robustness of the result across estimation strategies supports the conclusion that IGO membership plays a meaningful role in the diffusion of national cybersecurity strategies.

6 Potential Text-Based Analyses of National Cybersecurity Strategies

To illustrate the kinds of future research questions that can be explored with the text data specifically, we begin with some basic descriptive inquiries—for example: What are the main "buzzwords" used by countries in their national cybersecurity strategies (NCS)? And have these buzzwords changed over time? While our purpose here is not to conduct a full content analysis, we created a series of word clouds to visually demonstrate how language in national strategies has evolved.

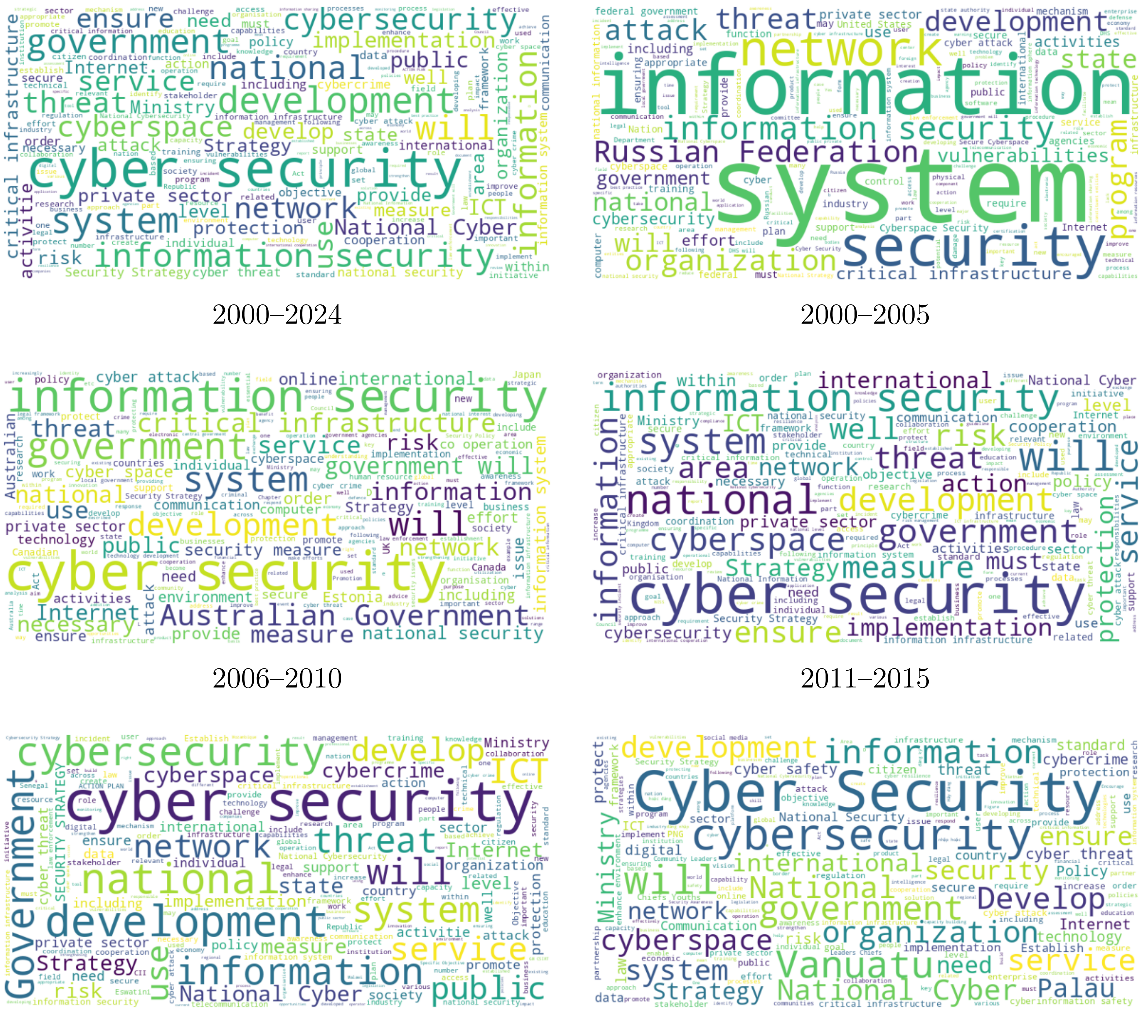
To do this, we grouped all inaugural NCS documents by the year of their adoption, roughly into five-year periods: 2000–2005, 2006–2010, 2011–2015, 2016–2020, and 2021–2024. Table 5 shows which countries fall into each period, revealing significant variation in the number and distribution of strategies across time. We then used the full text of strategies within each period to generate word clouds. In a word cloud, the size of each word reflects its frequency or prominence in the underlying text—larger words appear more often, while smaller words are less frequently used. In this case, the size of each term reflects how commonly it appeared in the strategies adopted during a given period.

Figure 3 presents the resulting word clouds. These word clouds suggest several notable trends. One example that we decided to focus on here is the evolution of the terms "cyber security" and "information security." The term *cyber security*—more commonly used by Western countries—tends to reflect a narrower, more technical understanding of digital security, often focused on the CIA triad (confidentiality, integrity, availability). By contrast, *information security*—favored in countries like Russia and China—encompasses a broader set of concerns, including political and ideological dimensions.

[6] We also explored categorizing the IGO variable into bins and including it as a factor in the model, but these specifications failed to resolve convergence or separation issues.

Table 5: Adoption of an Inaugural National Cybersecurity Strategy by Country Year

Period	***Total Docs***	***Countries (Years)***
2000–2005	4	Philippines (2005), Russia (2000), Tajikistan (2003), USA (2003)
2006–2010	6	Japan (2006), Canada (2010), United Kingdom (2009), Estonia (2008), Australia (2009), Malaysia (2006)
2011–2015	44	Ghana (2015), Lithuania (2011), South Korea (2011), Saudi Arabia (2013), Jamaica (2015), Georgia (2012), Montenegro (2013), Austria (2013), Iceland (2015), Finland (2013), Qatar (2014), Czech Republic (2011), Nigeria (2014), Moldova (2015), Switzerland (2012), Kenya (2014), Hungary (2013), Poland (2013), Botswana (2015), Jordan (2012), Rwanda (2015), Italy (2013), Trinidad and Tobago (2012), Bangladesh (2014), Afghanistan (2014), Mauritius (2014), South Africa (2015), Croatia (2015), Albania (2015), Slovakia (2015), Norway (2012), Netherlands (2011), Turkey (2013), Cyprus (2012), New Zealand (2011), Romania (2013), Ireland (2015), Germany (2011), Colombia (2011), Denmark (2014), Spain (2013), Uganda (2014), Malta (2015), India (2013)
2016–2020	36	Sierra Leone (2016), North Macedonia (2018), Lebanon (2019), Belize (2020), Sri Lanka (2018), Indonesia (2017), Costa Rica (2017), Thailand (2017), Samoa (2016), Gambia (2020), Tanzania (2016), Malawi (2017), China (2016), Serbia (2017), Greece (2018), Liberia (2017), UAE (2017), Egypt (2017), Eswatini (2020), Nepal (2016), Sweden (2017), Kiribati (2020), Belarus (2019), Israel (2017), Armenia (2017), Bulgaria (2016), Slovenia (2016), Mozambique (2016), Senegal (2017), Seychelles (2019), Chile (2017), Singapore (2016), Bahrain (2017), Kuwait (2017), Mexico (2017), Antigua and Barbuda (2018)
2021–2024	7	Papua New Guinea (2024), Pakistan (2021), Zambia (2021), Vanuatu (2021), Ethiopia (2021), Palau (2022), Vietnam (2022)



2000–2024

2000–2005

2006–2010

2011–2015

2016–2020

2021–2024

Figure 3: Word Clouds by Period Based on National Cybersecurity Strategy Documents

The first word cloud aggregates all 97 English-language NCS documents published between 2000 and 2024. Here, we already see "cyber security" appearing slightly larger than "information security," suggesting it is the more frequently used term across the full corpus. Looking at this evolution over time, the earliest word cloud (2000–2005), based on strategies from Russia, Tajikistan, the Philippines, and the United States, shows that *information security* dominates the discourse—a reflection of its use across all four documents. In the 2006–2010 period, with six strategies adopted, the term *cyber security* becomes more prominent, indicating a potential shift in terminology. This trend continues in subsequent periods. The word clouds for 2011–2015, 2016–2020, and 2021–2024 all show a growing emphasis on *cyber security.* This evolution might reflect two things: (1) the increasing adoption of the term by Western countries and/or (2) a broader global shift toward a narrower, more technical framing of cybersecurity. One valuable line of future research would be to assess whether this shift in terminology reflects a greater number of strategies being adopted by Western-aligned countries, or whether it suggests a global convergence toward the *cybersecurity* framing—even among states previously aligned with a broader *information security* paradigm.

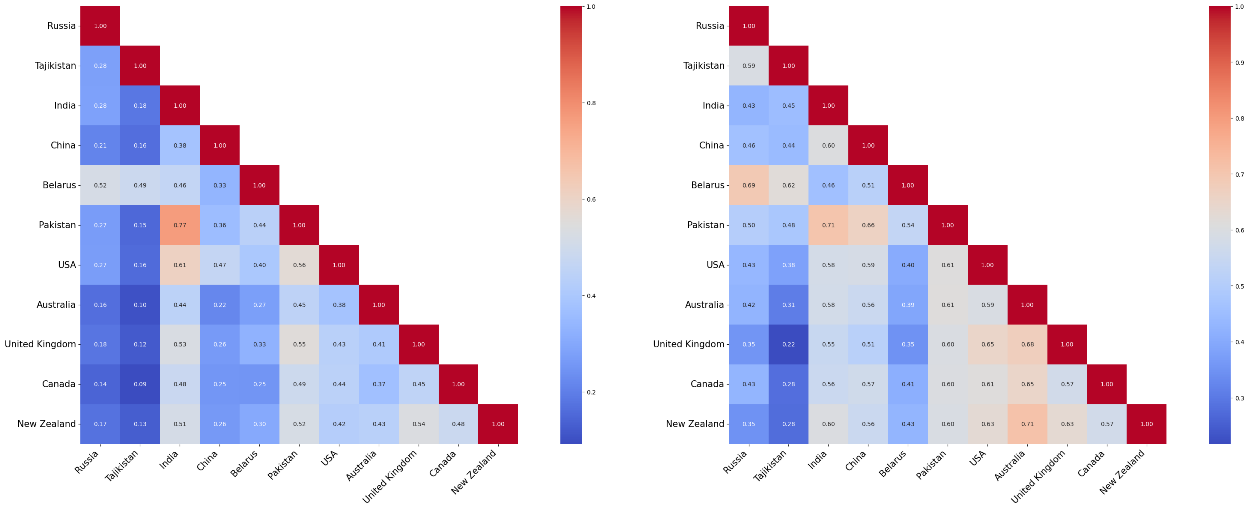
Another important question researchers can explore is: Do states emulate each other when crafting national cybersecurity strategies? To investigate this, we conduct a descriptive analysis using two types of document similarity measures: Term Frequency–Inverse Document Frequency (TF-IDF) cosine similarity and semantic embedding cosine similarity.

We focus on the inaugural national cybersecurity strategies of countries from the Five Eyes alliance and the Shanghai Cooperation Organization (SCO)—specifically those for which English-language versions are available. These countries were chosen because they represent a mix of allies and adversaries, allowing us to observe whether these relationships are reflected in the textual structure of their strategies.

Figure 4a shows the results based on TF-IDF cosine similarity. A higher score indicates that two documents share keywords that are both frequent in each document and relatively rare across the entire corpus. In simpler terms, TF-IDF captures surface-level lexical similarity—documents that use the same words in similar ways. Since TF-IDF primarily captures word overlap, it may underestimate similarity when countries use different vocabularies to express similar ideas. Consequently, Five Eyes countries do not appear particularly similar in terms of TF-IDF scores, while certain SCO countries—like India–Pakistan (0.77) and Russia–Belarus (0.52)—show higher overlap.

Figure 4b presents results based on semantic embedding cosine similarity, where documents are transformed into dense vectors using a pre-trained language model. This method captures context, word order, and semantic meaning, making it better suited for analyzing nuanced or paraphrased texts. Here, the similarity scores are generally higher than with TF-IDF, and many of the same closely linked pairs re-emerge: India–Pakistan (0.71), Belarus–Russia (0.69), and China–Pakistan (0.66). The Five Eyes countries also show stronger alignment in this model: USA–UK (0.65), Australia–New Zealand (0.71), and Canada–USA (0.61).

Overall, semantic embeddings reveal greater coherence within the Five Eyes, while SCO countries show more variability, albeit with strong connections among certain pairs. These findings suggest that textual similarity may reflect geopolitical alignment, though the extent and nature of this reflection vary depending on the method used and requires further testing.



(a) TF-IDF Cosine Similarity

(b) Semantic Embedding Cosine Similarity

Figure 4: Cosine Similarity of Inaugural National Cybersecurity Strategies Among Selected Countries

References

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.

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.

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.

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