Data & Policy (2025), 7: e7
doi:10.1017/dap.2024.99

RESEARCH ARTICLE

Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons

Hasan Çifci[1] and Esma Ergüner[2]

[1]İstanbul Aydın Üniversitesi, Küçükçekmece/İstanbul, Türkiye
[2]Başkent Üniversitesi, Etimesgut/Ankara, Türkiye
Corresponding author: Esma Ergüner; Email: eeozkoc@baskent.edu.tr

Received: 13 October 2024; **Revised:** 26 November 2024; **Accepted:** 14 December 2024

Keywords: comparative analysis; cybersecurity; G20 countries; national cybersecurity strategy; topic modeling

Abstract

This study analyzes National Cyber Security Strategies (NCSSs) of G20 countries through a novel combination of qualitative and quantitative methodologies. It focuses on delineating the shared objectives, distinct priorities, latent themes, and key priorities within the NCSSs. Latent dirichlet allocation topic modeling technique was used to identify implicit themes in the NCSSs to augment the explicitly articulated strategies. By exploring the latest versions of NCSS documents, the research uncovers a detailed panorama of multinational cybersecurity dynamics, offering insights into the complexities of shared and unique national cybersecurity challenges. Although challenged by the translation of non-English documents and the intrinsic limitations of topic modeling, the study significantly contributes to the cybersecurity policy domain, suggesting directions for future research to broaden the analytical scope and incorporate more diverse national contexts. In essence, this research underscores the indispensability of a multifaceted, analytical approach in understanding and devising NCSSs, vital for navigating the complex, and ever-changing digital threat environment.

Policy Significance Statement

This research presents valuable insights and vision for policymakers by examining G20 nations' National Cyber Security Strategiesusing a combination of qualitative and quantitative analysis. The study provides a broad understanding of cybersecurity dynamics of developed countries through a detailed analysis of shared goals, distinct focus areas, and underlying themes in their cybersecurity strategy documents. By using topic-modeling algorithm to uncover implicit focus items and themes, the findings reveal unstated policy statements to show the broader strategic landscape. Policymakers can use this analysis to address both common and country-specific cybersecurity challenges by considering widely adopted strategies in the developed states. Such an effort by policymakers will contribute international cooperation and policy alignment in cybersecurity domain.

1. Introduction

The study of National Cyber Security Strategies (NCSSs) has attracted significant academic attention due to their influential role in shaping national cybersecurity policies and practices. Studies related to NCSSs can be classified as (i) country-based studies that produce outputs contributing to the development, revision, or in-depth examination of their own NCSSs (Montasari, 2023), and (ii) studies focused on the

comparative analysis of specific countries' NCSSs to identify differences and similarities (Iova and Watashiba, 2023). The countries involved in such studies can be members of any union (EU, NATO, BRICS, etc.) or can often be selected countries that are thought to have more developed NCSSs (Ovchinnikova and Upadhyay, 2023; Štitilis et al., 2017; Newmeyer, 2015; Sabillon et al., 2016; Shafqat and Masood, 2016; ITU, 2018a, 2018b; OECD, 2012; Luiijf et al., 2013).

We focused on the NCSSs of the G20 countries since they represent the majority of the world's economy and population. Additionally, the diversity within the G20 in terms of information technology infrastructure and cybersecurity policies adds significant values for strategy analysis. Therefore, examining the G20's cybersecurity policies offers important new perspectives on global trends, priorities, and prospective areas for future international collaboration.

To understand the cybersecurity strategies of G20 countries we tried to find the answers to the following research questions (RQ):

RQ1: What are the shared objectives and distinct priorities of G20 cybersecurity strategies?

RQ2: What are the latent themes in G20 cybersecurity strategies, as revealed by topic analysis, but not explicitly stated in the strategy documents?

RQ3: What are the predominant and common keywords in G20 cybersecurity strategies?

To answer these research questions, we used a mix of qualitative and quantitative approaches by utilizing expert visions and advanced analytical techniques. A sophisticated machine learning technique called topic modeling was used as quantitative analysis to uncover latent themes and patterns. Together with qualitative analysis, topic modeling provided a unique and objective way to interpret the complex nature of global cybersecurity strategies.

In the literature, there are studies comparing NCSSs of countries and international alliances. Most of the analysis is qualitative, that is primarily based on expert analysis while few using quantitative methods such as topic modeling. This study is the most recent analysis in the domain since it incorporates the newest versions of national cybersecurity strategies. Whereas previous studies mostly focused on discovering thematic similarities or common issues, our study goes further by revealing shared objectives, distinct priorities, latent themes, and new trends in the strategies.

The findings of the study present vital information for cybersecurity community about cybersecurity strategies to develop better-informed and globally aligned strategies. The comparative analysis of the G20 countries' strategies also helps to improve awareness of common cybersecurity trends that have influence on future policies in this essential domain.

2. Literature review

Around the world, governments developed strategies to deal with problems in digital security, stop threats, reduce risks, prevent attackers, and make sure their digital systems are strong and safe to help progress in business, technology and society (ITU, 2018a; ENISA, 2016). Organizations such as International Telecommunication Union (ITU), European Union Agency for Cybersecurity (ENISA), Organization for Economic Co-operation and Development (OECD), NATO, and Oxford University have shared guidance resources to support nations in building good cybersecurity strategy and plans. Table 1 presents the most common cybersecurity indices and frameworks that can be used as guidance to develop NCSSs.

National Cybersecurity Strategies are usually revised and updated about every four to six years (United Nations, 2024a). This periodic update process is necessary for adapting to the continually changing landscape of cyber threats and advances in technology. Given the natural cycle of renewal, our literature review began with studies published from 2018 onwards.

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

Table 1. *Common National Level Cybersecurity indices and frameworks*

Year	Name	Reference
2011	Cyber Power Index (Economist)	EUI & Booz Allen Hamilton (2011)
2011	ITU National Cybersecurity Strategy Guide	Wamala (2011)
2012	National Cyber Security Strategies	ENISA (2012a)
2012	National Cyber Security Strategies-Practical Guide on Development and Execution	ENISA (2012b)
2012	National Cyber Security Framework Manual	NATO CCD COE (2012)
2012	Cybersecurity Policy Making at a Turning Point	OECD (2012)
2013	The Cyber Index-International Security Trends and Realities	UNIDIR (2013)
2014	An Evaluation Framework for National Cyber Security Strategies	ENISA (2014)
2015	Cyber Readiness Index (CRI)	Potomac Institute for Policy Studies (2015)
2016	NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies	ENISA (2016)
2018	Guide to Developing a National Cyber Security Strategy-Strategic Engagement in Cybersecurity	ITU (2018a)
2019	Good Practices in Innovation Under NCSS	ENISA (2019)
2020	National Cyber Power Index (NCPI)	Belfer Center for Science and International Affairs (2020)
2020	National Capabilities Assessment Framework (NCAF)	ENISA (2020)
2021	Cyber Capabilities and National Power	IISS (2021)
2021	Cybersecurity Capacity Maturity Model for Nations (CMM)	Oxford GCSCC (2021)
2024	Global Cybersecurity Index (GCI)	ITU (2024)
2024	National Cyber Security Index (NCSI)	e-Governance Academy (2024)

Azmi et al. (2018) analyzed widespread cybersecurity frameworks using document analysis and identified shared actions, pillars, and lifecycle processes to present a general model for organizations and governments. Sunkph et al. (2018) examined the implementation of international cybersecurity policies in ASEAN (Association of Southeast Asian Nations) countries (Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam) and highlighted the importance of regional collaboration to address escalating cyber threats. Gorka (2018) analyzed the aims of the NCSSs of Visegrad Group (Czechia, Poland, Slovakia, and Hungary) to reveal similarities and differences among these states.

Kovacs (2019) analyzed the cyber security strategies of the EU, NATO, and four EU countries (Austria, Czechia, Hungary, and the UK) to determine possible elements and conclusions of the strategies. Baezner and Cordey (2019) compared the cybersecurity strategies of six European countries and identified eight shared challenges, including similarities and differences in their approaches.

Enescu (2020) analyzed EU member states' cybersecurity strategies and highlighted their alignment with EU initiatives and areas of divergence. Santisteban et al. (2020) analyzed 20 NCSSs to determine the strategies of mostly targeted nations in the cyber domain. Handbook of International Cybersecurity (Tikk and Kerttunen, 2020) presents various perspectives on international cybersecurity and covers cybersecurity concepts and frameworks, national and regional strategies, and global approaches to cybersecurity.

Jacuch's study (2021) compared the cybersecurity strategy of Poland and those of five other nations: the UK, the US, France, Lithuania, and Estonia. He examined strategic documents from these countries to identify key similarities and differences to provide recommendations for strengthening Poland's

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

cybersecurity framework. In another study to audit national strategies, Sabillon (2021) examined the best practices of 10 major countries in terms of building effective cybersecurity strategies and policies.

The Organization of American States (OAS) (2022) analyzed the cybersecurity strategies of its 35 member states and compared approaches and common challenges. Falch et al. (2023) focused on the Nordic-Baltic region and compared strategies in terms of threat assessments, risk management, and international cooperation. Odebade and Benkhelifa (2023) conducted a comparative study of the NCSSs of 10 nations across Europe, Asia-Pacific, and North America. They found a common emphasis on protecting critical infrastructure to improve public-private partnerships. Ali et al. (2024) use various analysis techniques for evaluating and improving cybersecurity posture of countries. The study compares the cybersecurity of underdeveloped countries (Pakistan) against developed countries (Lithuania, Estonia, Singapore, Spain, and Norway) and suggests frameworks and recommendations.

Topic modeling is increasingly being used for cybersecurity from malware detection to document analysis (Bechor and Jung, 2019; Samtani et al., 2016). Adams et al. (2018) utilized topic modeling to analyze textual descriptions of attack patterns and estimate topic distributions to help experts with attack evaluations. Bechor (2019) explored the intersection of cybersecurity and data science by applying LDA topic modeling to scholarly articles published between 2012 and 2018. Ignaczak et al. (2022) systematically reviewed 83 studies to propose a taxonomy of cybersecurity activities supported by text mining and topic modeling. Barik et al. (2022) conducted a systematic literature review (SLR) on the use of text mining in cybersecurity and analyzed 516 papers published between 2015 and 2021. They emphasized the potential of text mining methods to contribute to and improve cybersecurity efforts.

One of the first studies of topic modeling used to analyze the similarities and differences between NCSSs can be attributed to Kolini and Janczewski (2017). They gathered and evaluated 60 NCCSs that were created between 2003 and 2016. Additionally, they suggested that the topic modeling approach can be utilized as an automated way for textual analysis and evaluation of national strategies. Song et al. (2021) employed topic modeling to analyze the NCSSs of the US, UK, Japan, and the EU to discover the policy changes over time and to revise South Korea's NCSS.

Even though the prior studies contributed to the literature by analyzing NCSSs, there is a significant gap regarding the detailed analysis of G20 nations' strategies, both qualitatively and quantitatively. Previous research was often focused on specific regions or groups of countries such as ASEAN countries (Sunkph et al., 2018), the Visegrad Group (Gorka, 2018), or selected European nations (Baezner and Cordey, 2019; Kovacs, 2019). Among the research that used topic modeling, the study by Song et al. (2021) focused on the US, UK, Japan, and the EU only for policy changes over time and Kolini and Janczewski (2017) analyzed NCSSs up to 2016, but their study did not focus on the G20 nations and is now outdated, as NCSSs have since been updated. In short, the literature lacks analyses of shared perspectives, distinct priorities, and latent themes in current G20 cybersecurity strategies. To address these gaps in the literature, we formulated research questions as presented in the introduction section of this manuscript.

3. Materials and methods

This study contains 10 primary steps as shown in Figure 1.

Initially, we sourced the NCSS documents for all G20 countries on the internet. For NCSS documents not in English, specifically those from Brazil and China, we utilized Google Translate for translation.

Explicitly stated objectives in strategy documents were then extracted manually by reading the documents. The set of declared cybersecurity goals and priorities of each G20 nation was obtained after this step.

To discover implicit themes and priorities within these strategies, we created Python code for topic analysis using latent dirichlet allocation (LDA). We chose LDA algorithm since it is widely used effective topic modeling algorithm to uncover hidden themes or topics within a set of documents (Blei et al., 2003). Each document was analyzed separately as its own corpus to reflect its unique context with lengths ranging from 2500 words to 32,000 words and this is sufficient data for meaningful topic modeling. We adjusted the number of topics based on the explicit themes found in each document to match its content. With this approach, we avoided choosing the number of topics randomly. The code was written in Python

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

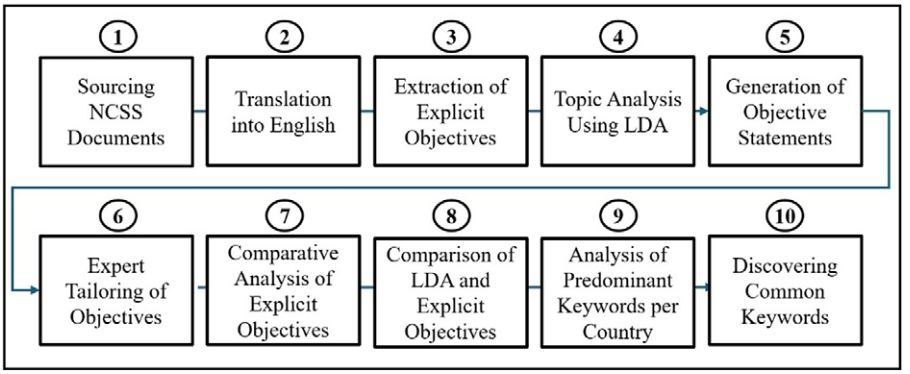

Figure 1. *Study steps.*

using NLTK and Gensim libraries. The text was prepared by tokenizing and lemmatizing, removing stop words, and filtering out non-alphabetic words. By using LDA, we were able to go beyond a simple keyword analysis and uncover the latent themes and objectives in G20 cybersecurity strategies.

After employing the LDA topic modeling algorithm on each strategy document, we identified topics consisting of sets of keywords with associated weights. To create meaningful statements from these keywords, we used the GPT-4 advanced language model (OpenAI 2024). In other words, LDA-generated keywords with their weights were given into GPT-4 to generate preliminary topic statements for each country. Since the context of NCSSs has nuances that could be misled by an AI model, we reviewed and revised the GPT-4 generated topic statements. With this iterative process, we generated and then revised latent topics to ensure they accurately reflected the context of each country's strategy.

Now then, we had all the data to start with the detailed analysis of the strategies. We first performed an analysis to compare explicitly stated objectives in the G20 strategies. Then we analyzed the implicit objectives of the strategies discovered by topic modeling. With the help of these two different analyses, we obtained comparisons of explicit and implicit objectives and unstated latent focus areas and concerns of the G20 countries.

Furthermore, we analyzed the predominant keywords of the strategies, extracted from LDA topics, to get information about the focal areas and thematic emphasis within each nation's cybersecurity policy.

Lastly, we identified common keywords in the strategies, extracted from LDA topics. This step was important to understand the common focus areas of the strategies.

4. Findings and results

In this section, we provided the research questions and their answers.

RQ1: Shared objectives and distinct priorities in G20 cybersecurity strategies

We extracted the objective statements manually from the G20 strategies. We found that there are 25 distinct objectives as shown in Table 2 (Argentina Government, 2023; Australian Government, 2020; Brasil Presidency of the Republic, 2020; Government of Canada, 2018; The Cyberspace Administration of China, 2016; European Commission, 2020; ANSSI, 2015; German Federal Ministry of Interior, 2016; Indian Ministry of Communication and IT, 2013; Indonesian Government, 2023; Italian Government, 2022; Government of Mexico, 2017; Japanese Government, 2021; Russian Federation, 2016; Kingdom of Saudi Arabia, 2020); South Korea National Security Office, 2019; Republic of Turkey, 2020; UK Government, 2016; The White House, 2023; South Africa State Security Agency, 2012). The objectives are organized based on the number of their adoptions by these countries.

The most widely accepted objectives, adopted by 10–17 countries, include protecting critical infrastructures, networks, and data; establishing national coordination and ecosystems; engaging in

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

Table 2. *Objectives in the NCSSs of G20 countries*

No	Objective	Countries	#[1]
1	Protect critical infrastructures, networks, and data	ARG, AUS, BRA, CAN, CHN, EU, FRA, DEU, IND, IDN, ITA, MEX, RUS, KOR, TUR, UK, USA	17
2	Establish national coordination and ecosystem	AUS, BRA, CAN, EU, DEU, IND, ITA, JPN, MEX, SAU, ZAF, KOR, UK, USA	14
3	Engage in international cooperation	ARG, BRA, CHN, EU, FRA, DEU, IDN, JPN, ZAF, KOR, TUR, UK, USA	13
4	Support cybersecurity industry, R&D (Research & Development) and innovation	ARG, AUS, BRA, CAN, EU, IND, MEX, SAU, ZAF, KOR, UK	11
5	Enhance cybersecurity capabilities	AUS, CHN, EU, IDN, ITA, JPN, MEX, SAU, TUR, UK	10
6	Raise awareness and foster cybersecurity culture	ARG, AUS, BRA, CHN, FRA, IND, ZAF, KOR	8
7	Establish incident response capacity	ARG, EU, IND, IDN, ITA, RUS, SAU, KOR	8
8	Address cyber crime	AUS, CHN, EU, JPN, MEX, ZAF, TUR, USA	8
9	Establish legislative and regulatory framework	ARG, BRA, EU, IND, IDN, ITA, ZAF	7
10	Provide secure products and services	ARG, AUS, FRA, IND, MEX, UK	6
11	Establish a clear governance structure	BRA, CHN, IDN, SAU, ZAF	5
12	Set effective deterrence capabilities	EU, JPN, RUS, UK, USA	5
13	Provide information sharing	AUS, EU, IND, JPN	4
14	Grow a skilled workforce	AUS, IND, ZAF, UK	4
15	Respect individual rights and fundamental values	CAN, EU, FRA	3
16	Security of new generation technologies	EU, TUR, UK	3
17	Encourage use of and compliance with open and international standards	EU, IND, ZAF	3
18	Integrate cybersecurity into national security and sovereignty	CHN, MEX, TUR	3
19	Improve cybersecurity supply chain	IND, JPN	2
20	Improve military information systems security	EU, RUS	2
21	Promote interests of allies in cyberspace	RUS, USA	2
22	Countervailing information and psychological actions	RUS	1
23	Foster national and domestic technologies	TUR	1
24	Take the lead in the technologies vital to cyber power	UK	1
25	Disrupt and dismantle threat actors	USA	1

[1]Shows the number of countries which have those keywords.

international cooperation; supporting cybersecurity industry, R&D, and innovation; and improving cybersecurity capabilities. The acceptance of these objectives demonstrates widespread agreement about the significance of holistic cybersecurity measures, collaborative frameworks, and innovative

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

developments in this domain. These shared objectives among G20 countries indicate a unified approach to cybersecurity.

Among the shared objectives, emphasis on international cooperation shows a recognition that cyber threats require collective actions. For example, the Budapest Convention on Cybercrime is referenced in several strategies and most of the G20 countries, except for Russia, China, India, Indonesia, and Saudi Arabia, are among the signatory bodies (Council of Europe, 2024). Nations like the USA, UK, and EU members actively participate in international organizations and adopt common standards such as ISO/IEC 27000 series and the NIST Cybersecurity Framework, and GDPR (General Data Protection Regulation) (European Union, 2024). For collaboration, there are various global cybersecurity initiatives and alliances that G20 nations are among the members, such as ENISA (2024), ASEAN (2024), GFCE (Global Forum on Cyber Expertise) (2024), FIRST (Forum of Incident Response and Security Teams) (2024), UN GGE (United Nations Group of Governmental Experts) (United Nations, 2024b), The Paris Call for Trust and Security in Cyberspace (Paris Call 2024), and APEC (Asia-Pacific Economic Cooperation) Cybersecurity Strategy (APEC, 2005). Despite these efforts, because of the different national interests, legal systems, priorities, and technological advancements, challenges remain in widespread cooperation.

Moderately adopted objectives, adopted by 5–8 countries, are raising awareness, and fostering cybersecurity culture, establishing incident response capacity, addressing cybercrime, establishing legislative and regulatory frameworks, and providing secure products and services. These objectives reflect a focus on specific aspects of cybersecurity, such as legal structures, public education, and incident management, which are crucial but perhaps not as universally prioritized as those in the most adopted category.

Selectively adopted objectives, adopted by 3–4 countries, include respecting individual rights and fundamental values, security of new generation technologies, and encouraging the use of international standards. This suggests a more targeted approach to cybersecurity, possibly addressing unique national challenges or focusing on emerging areas in cybersecurity.

In the cybersecurity strategies of G20 countries, certain objectives, adopted by 1–2 countries, demonstrate unique national focuses. India and Japan prioritize the security of the supply chain. The European Union and Russia, on the other hand, emphasize the security of their military information systems. Russia and the USA demonstrate a cross-national strategy by focusing on expanding cybersecurity protection to include the interests of their respective allies. Exclusively, Russia addresses the contemporary aspect of cyberwarfare, which is the task of blocking disinformation and psychological operations online. Turkey shows a dedication to self-reliance and innovation by focusing its efforts on the development of domestic and national cybersecurity solutions. With a unique positioning in crucial cyber technologies, the UK aims to gain a strategic advantage in this quickly changing industry. Finally, to emphasize its commitment to active warfare in the digital domain, the USA takes a proactive and aggressive posture and focuses on the disruption and dismantling of cyber threat actors. These goals show the variety of approaches that the G20 countries have been using, each customizing their strategy to fit unique national interests and security concerns in the global cyber landscape.

RQ2: Latent themes in the cybersecurity strategies of G20 countries

We created Python code to use LDA topic modeling algorithm to uncover latent themes in G20 cybersecurity strategies. LDA algorithm generated topics for each of the strategy documents. There are sets of keywords in the topics with weights that show the importance of the keywords in the entire strategy document. Then, GPT-4 was used to create meaningful statements from each topic to create coherent and interpretable topics. Since there is a potential that AI-generated content might miss the context-specific meanings, we revised the GPT-4 generated statements manually. The process was iterated for each G20 country. This expert revision ensured that the final topic descriptions adequately captured the thematic meaning of the LDA-generated themes. A sample topic's process is shown below:

(1) LDA topic from Australia's strategy document: 0.146*'critical' + 0.096*'national' + 0.072*'asset' + 0.069*'need' + 0.044*'invest'. (Note that, the weights indicate how strongly each word contributes to the topic definition.)

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

(2) GPT-4 generated statement: "Investing in national assets is critical due to the need for robust infrastructure and security."
(3) To ensure contextual relevance and accuracy, we reviewed and revised these generated statements manually. Expert revised statement: "Investing in critical national assets is needed for robust infrastructure and security."

After discovering latent objectives in the strategies, we performed a comparison process to see which of the implicit objectives were not stated explicitly in the strategies. With this comparison, we found areas of implicit focus or unspoken objectives that influence these countries' cybersecurity postures and priorities. The comparative study revealed that while all explicitly stated objectives were discovered by LDA analysis, there are latent topics that are not explicitly stated in the strategies. See Table 3 for implicit strategic concerns of G20 strategies.

Table 3. *Topics found by LDA but not explicitly stated in the strategy documents*

Country	Latent topics
ITA	Supporting international initiatives.
	Fostering public-private partnerships.
	Promoting cybersecurity awareness and education.
RUS	Countering threats through international cooperation.
	Prioritizing security provision within its legal framework.
	Addressing problems arising from foreign interactions and emphasizing intelligence.
CHN	Protection of global digital rights.
	Innovation within cyberspace, investing in cutting-edge technologies.
	Developing and enforcing laws to regulate activities in cyberspace.
MEX	Collaborating with institutions, the private sector, and entities to advance national cybersecurity.
	Educating individuals and society and improving digital security awareness.
SAU	Adhering to international standards.
ZAF	Focusing on critical departments and technology sectors within the state.
	Protecting the Republic's telecommunication infrastructure.
IND	Empowering society in a digital environment.
	Focusing on the development and implementation of secure software.
DEU	Investing in cybersecurity defensive technologies.
	Enforcement of national laws
AUS	Reinforcing AUS's position as a leader in the digital space.
BRA	Respecting citizens' information privacy.
CAN	Investments in quantum computing technologies.
JPN	Promoting private sector participation in national cybersecurity initiatives.
KOR	Protecting businesses and citizens' rights and data.
EU	Investing in research tools and processes that drive societal development and contribute to the Union's annual growth and cost-effectiveness.
IDN	Providing a legal basis for digital interactions.
ARG	None.
FRA	None.
TUR	None.
UK	None.
USA	None.

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

The analysis revealed that G20 countries reflect following perspectives in their strategies indirectly:

- Dynamics of cybersecurity is global and there is a need for international collaboration.
- There is an interest in technological innovation and advancing cybersecurity technologies.
- There is an awareness of legal and regulatory considerations that shows the need for legal frameworks.
- Public-private partnership is vital to improving national cybersecurity initiatives.
- Critical infrastructures and services have to be protected against cyber attacks.
- Privacy and data protection should be addressed.
- Education and workforce development is vital to have a skilled cybersecurity workforce and raise public awareness of cyber threats.

The findings from the LDA analysis provide understanding of the diverse approaches nations use to maintain the balance between explicit and implicit declarations of cybersecurity strategies.

RQ3: Predominant and common keywords in the G20 cybersecurity strategies

Keywords were found by using LDA technique. We excluded common keywords such as "national ""cyber ""security ""cybersecurity ""cyberspace "and "strategy" from the keywords pool. This enabled us to move our focus away from these commonly used but generic terms and onto more distinctive and specialized components of each country's approach. These common keywords while important frequently mask the subtle distinctions between countries.

During analysis, the top 50% of keywords by weight from each country's strategy were involved, while concurrently limiting the number of keywords to a range of 15–20. This approach was chosen to ensure both depth and breadth in our analysis, capturing a vast array of significant terms without overwhelming the focus on the most crucial elements. By implementing a percentage threshold, we maintained consistency across datasets of varied sizes, thus accommodating the inherent variability in the volume and detail of the original strategy documents. The additional constraint of 15–20 keywords was important in preventing over- or under-representation, thereby guaranteeing a focused but encompassing description of each country's strategic priorities.

Following the extraction of keywords from LDA topics, we arranged them according to their respective weights, ensuring an accurate representation of their significance within the cybersecurity strategies of each country. Top keywords and priorities of the G20 countries are given in Table 4.

Apart from keywords such as "national," "cyber," "security," "cybersecurity," "cyberspace," and "strategy," there are 66 common keywords (again generated by LDA topic modeling) that exist in the strategies of at least two countries as shown in Table 5. To prevent the table from extending across multiple pages, keywords that occurred with the same frequency across different countries were consolidated into a single row. The countries where each keyword appeared were enclosed in curly brackets ({}) to indicate the specific nations associated with that keyword.

The analysis revealed a universal emphasis on 'Information', appeared in the strategies of 18 countries, underscoring information as a vital aspect of cybersecurity.

Furthermore, the concurrent prominence of 'Government' and 'Technology' in 12 countries' strategies may reflect an integration of state-driven policies and technological advancements in cybersecurity. This trend might show growing recognition of the need for governmental intervention in cybersecurity and investments in the technological domain to support national cyber defenses. Additionally, 11 countries have 'Development' and 'International' keywords that can show a motivation for developing robust cybersecurity posture and improving international cooperation.

The existence of 'Sector', 'System', and 'Threat' in 10 countries might denote a focus on specific sectors, systemic security and threats. The keyword 'Service', in nine countries may indicate a service-oriented approach to cybersecurity. Having 'Digital', 'Private', and 'Public' keywords in seven countries may show the collaboration of both private and public sectors in cybersecurity efforts.

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

Table 4. *Top keywords in G20 cybersecurity strategies*

Country	Top keywords (ordered in weights)
ARG	Information, Sector, International, Organization, Development, State, Objective, Public, Private, Framework, Society, Detection, Protection, People, Republic
AUS	Government, Business, Critical, Information, Threat, Service, Technology, Crime, Community, Infrastructure, Support, Capability, Action, Malicious, Industry, Advice, Protect, Online, Incident, Sector
BRA	Training, Sector, Public, Information, Private, Action, Technology, Country, Program, International, Data, Society, Institution, Government, Communication, Threat, Attack, Service, Resource, Protection
CAN	Information, Computer, Government, Network, Service, Digital, Threat, Data, Organization, System, Technology, Quantum, Malicious, Internet, World, Leadership
CHN	Network, Internet, Information, International, System, Country, Law, Improve, Development, Management, Promote, Strengthen, Governance, New, Cooperation, Construction
DEU	Federal, Government, International, Attack, Information, System, Digital, Law, Defense, Technology, Measure, Threat, Action, Process, New
EU	Member, Cooperation, Commission, Digital, Support, Internet, Information, Defense, Network, Building, International, Development, Authority, Rule, Agency, Joint, Technology, Action, Threat, Global
FRA	Digital, Service, State, Business, Product, System, Information, Technology, Data, International, Sector, Development, Support, Public, Trust, Education, Personal, Economic, Stakeholder, Private
IDN	Crisis, Implementation, Intended, Plan, Referred, Management, Development, Action, Incident, Agency, Information, Regulation, Electronic, Follows, Calculation
IND	Information, Infrastructure, Technology, Service, Development, Critical, Protection, Policy, Government, Create, Practice, Plan, Entity, Country, Sector, Management, Communication, Standard, Global, Product
ITA	Public, Digital, Development, Technology, Country, International, Administration, Private, Cooperation, System, Action, European, Response, Entity, Technical, Specific, Threat, Training, Initiative, Information
JPN	Information, Government, Effort, System, Measure, International, Service, Stakeholder, Collaboration, People, Work, Risk, Cyberattacks, Agency, Resource, Human
KOR	Government, International, Cooperation, Rule, Information, System, Strengthen, Practice, Business, Public, Goal, Right, Policy, Attack, Citizen
MEX	Information, Development, Public, State, Institution, Infrastructure, Private, Government, Threat, Sector, Asset, Risk, Internet, Entity, Telecommunication, Action, Technology, Protection, Digital, Individual
RUS	Information, Organization, System, Activity, State, Ensuring, Development, Government, Citizen, Threat, Field, Implementation, Strategic, Technology, Interaction, International, Problem, Force, Operation, Doctrine
SAU	Framework, Growth, Strategic, Goal, Vision, Achieve, Organization, Sector, Risk, Development, Private, Information, Threat, Track, Responsibility, Role, Ecosystem, Initiative
TUR	Action, Plan, Institution, Technology, Infrastructure, Activity, Critical, Public, International, Country, Developing, Organization, Determined, Stakeholder, Responsible, Measurement, Information
UK	System, Government, Service, Technology, Network, Information, Digital, Organization, Support, Threat, Data, Sector, Crime, Regulation, Capability, Incident, Software, Resilience, International, Infrastructure

(Continued)

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

Table 4. *Continued*

Country	Top keywords (ordered in weights)
USA	Federal, State, Effort, Government, Digital, Technology, Infrastructure, Sector, Partner, Critical, Private, Service, Support, Investment, Incident
ZAF	Information, Development, Sector, Policy, Government, State, Cybercrime, Framework, Implementation, Response, Critical, Role, Private, Communication, Technology, Cluster, Service, Measure, Infrastructure, Standard

Table 5. *Common keywords in G20 cybersecurity strategies*

Keywords	#	Countries
Information	18	ARG, AUS, BRA, CAN, CHN, EU, FRA, DEU, IND, IDN, JPN, MEX, RUS, SAU, ZAF, KOR, TUR, UK
Government, Technology	12	{AUS, BRA, CAN, DEU, IND, JPN, MEX, RUS, ZAF, KOR, UK, USA}, {AUS, BRA, CAN, FRA, DEU, IND, ITA, RUS, ZAF, TUR, UK, USA}
Development, International	11	{ARG, CHN, EU, FRA, IND, IDN, ITA, MEX, RUS, SAU, ZAF}, {ARG, BRA, CHN, EU, FRA, DEU, ITA, JPN, RUS, KOR, TUR}
Sector, System, Threat	10	{ARG, BRA, FRA, IND, MEX, SAU, ZAF, TUR, UK, USA}, {CAN, CHN, FRA, DEU, ITA, JPN, RUS, KOR, UK, USA}, {AUS, BRA, CAN, DEU, ITA, MEX, RUS, SAU, KOR, UK}
Service	9	AUS, BRA, CAN, FRA, IND, JPN, KOR, UK, USA
Digital, Private, Public	7	{CAN, EU, FRA, DEU, ITA, UK, USA}, {ARG, BRA, ITA, MEX, SAU, ZAF, USA}, {ARG, BRA, FRA, ITA, MEX, KOR, TUR}
Action, Critical, Organization, State	6	{AUS, BRA, DEU, IDN, ITA, TUR}, {AUS, IND, MEX, ZAF, TUR, USA}, {ARG, CAN, CHN, RUS, SAU, TUR}, {ARG, FRA, MEX, RUS, ZAF, USA}
Cooperation, Country, Implementation, Infrastructure, Support	5	{ARG, CHN, EU, ITA, KOR}, {BRA, CHN, IND, ITA, TUR}, {IDN, RUS, ZAF, KOR, USA}, {AUS, IND, MEX, TUR, USA}, {AUS, EU, FRA, UK, USA}
Cybercrime, Agency, Business, Data, Internet, Level, Network, New	4	{AUS, TUR, UK, ZAF}, {EU, IDN, JPN, USA}, {AUS, CAN, FRA, KOR}, {BRA, CAN, FRA, UK}, {CAN, CHN, EU, MEX}, {FRA, DEU, ITA, SAU}, {CAN, CHN, EU, UK}, {CAN, CHN, DEU, UK}
Attack, Communication, Entity, European, Federal, Framework, Incident, Institution,	3	{BRA, DEU, KOR}, {BRA, IND, ZAF}, {IND, ITA, MEX}, {EU, FRA, ITA}, {CAN, DEU,

(Continued)

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

Table 5. *Continued*

Keywords	#	Countries
Management, Plan, Policy, Protection, Risk, Strategic, Strengthen, Use		USA}, {ARG, SAU, ZAF}, {IDN, UK, USA}, {BRA, MEX, TUR}, {CHN, IND, IDN}, {IND, IDN, TUR}, {IND, ZAF, KOR}, {ARG, CHN, IND}, {JPN, MEX, SAU}, {RUS, SAU, TUR}, {ARG, CHN, KOR}, {ARG, CAN, DEU}
Activity, Area, Capability, Citizen, Defense, Effort, Goal, Law, Malicious, Measure, Objective, People, Practice, Promote, Regulation, Resource, Response, Responsibility, Right, Rule, Secure, Society, Stakeholder, Work	2	{RUS, TUR}, {BRA, RUS}, {AUS, UK}, {RUS, KOR}, {EU, DEU}, {JPN, USA}, {SAU, KOR}, {CHN, DEU}, {AUS, CAN}, {DEU, JPN}, {ARG, TUR}, {ARG, JPN}, {IND, KOR}, {ARG, CHN}, {IDN, UK}, {BRA, JPN}, {ITA, ZAF}, {SAU, ZAF}, {CHN, KOR}, {EU, KOR}, {AUS, USA}, {ARG, BRA}, {JPN, TUR}, {JPN, USA}

Figure 2. *Heatmap of Top 20 keywords weights by country.*

The presence of 'Action', 'Critical', 'Organization', and 'State' in six strategies might show a focus on active measures to protect critical infrastructure and organizational assets. Additionally, the presence of 'Cooperation', 'Country', 'Implementation', 'Infrastructure', and 'Support' in five countries' strategies may reflect a desire for implementation and support of cybersecurity infrastructure through cooperative efforts.

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

The mention of 'Cybercrime', 'Agency', 'Business', 'Data', 'Internet', 'Level', 'Network', and 'New' in four countries might reveal a focus on specific actions such as combating cybercrime, improving business value of cybersecurity, data security, and internet and network infrastructure. The inclusion of 'New' might mean mindset to adopt innovative approaches and technologies in cybersecurity measures.

Keywords that appear in three or two countries each can indicate an explicit focus on specific aspects of cybersecurity or context-based priorities in those countries.

Based on the analysis of the LDA topics, the heat-map in Figure 2 depicts the weights of the top 20 keywords in G20. Each cell's color intensity indicates the relative weight or significance of a specific keyword in a country's cybersecurity strategy.

5. Conclusion

In this study, a mixture of qualitative and quantitative methodologies was performed to explore the NCSSs of G20 countries. Through this rigorous analysis, we successfully discovered both the stated objectives and latent themes that are not stated explicitly within these strategies. Our findings reveal a complex tapestry of shared objectives and distinct national priorities among G20 countries in terms of cybersecurity strategies. Having shared objectives among the G20 nations is an indication of unified approaches in the strategies to strengthen cybersecurity.

The implementation of latent dirichlet allocation (LDA) for topic modeling played a significant role in discovering objectives and themes that were not visibly stated in the NCSS documents. This approach provided valuable insights into the implicit concerns and focus areas of different countries and therefore it enhanced our understanding of the strategic underpinnings of national cybersecurity policies. The analysis of predominant and common keywords further improved the understanding the nature and overarching trends in cybersecurity.

Our study's findings hold significant implications for cybersecurity policymakers at both national and international levels. By identifying shared objectives and latent themes among G20 countries, the insights gained can guide the formulation of more effective and contextually relevant cybersecurity policies. Policymakers can leverage common ground to strengthen international cooperation, adopt proven strategies against cyber threats and improve information sharing. Recognizing unique national strategies enables the development of customized strategies that address particular national problems while keeping up with worldwide cybersecurity trends. Additionally, the study highlights the critical need for continued and in-depth exploration of cybersecurity strategies to keep pace with the rapidly evolving cyber threat landscape.

However, this research is not without its limitations. The primary limitation is the analysis of NCSSs written in various languages, as translations may not capture the nuances and correct terminology of the original texts. All countries except for Brazil and China published English versions of their strategy documents, which minimizes the language limitation. Another limitation is the inherent constraints of algorithmic topic modeling. Normally, this limitation is inevitable while using topic modeling. On the other hand, to overcome this limitation, we manually analyzed the explicit strategies and manually revised the topics. Despite these challenges, the study contributes substantially to the field of cybersecurity policy analysis and offers a framework for future research endeavors that could expand to include a more diverse array of nations and employ more advanced analytical techniques.

For future research, there are some viable options to consider. Researchers could use multilingual semantic analysis tools to better capture the nuances of different languages. They could also explore other methods, such as dynamic topic modeling or deep learning, to gain deeper insights into how policies change over time. Additionally, future studies could focus on underexplored regions, analyze cybersecurity strategies in the private sector, or investigate how NCSSs are implemented and how effective they are across different countries.

In conclusion, our study underscores the importance of a multi-dimensional approach, containing both qualitative and quantitative methodologies, to understanding and developing national cybersecurity

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

strategies. As cyber threats continue to evolve in complexity and scale, such holistic analyses will be crucial in equipping nations to effectively safeguard their digital infrastructure.

Data availability statement. The data was collected from the G-20 countries' relevant websites publishing their cybersecurity strategies. Data is public.

Author contribution. Conceptualization: H.Ç.; E.E., Methodology: H.Ç., Literature search: H.Ç.; E.E., Draft preparation: H.Ç., Writing: H.Ç.;E.E All authors wrote the paper and approved the final submitted draft.

Funding statement. This work received no specific grant from any funding agency, commercial or not-for-profit sectors.

Competing interest. Author H.Ç. and Author E.E. declare none.

References

Adams S, **Carter B**, **Fleming C and Beling PA** (2018) Selecting system specific cybersecurity attack patterns using topic modeling. In *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*. IEEE, pp. 490–497. 10.1109/TrustCom/BigDataSE.2018.00076.

Ali SM, **Razzaq A**, **Abbass H**, **Yousaf M and Shan R us** (2024, October 18) A Hybrid Analytical Framework for Enhancing Cybersecurity in Underdeveloped Countries. In *2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*. https://doi.org/10.20944/preprints202410.1442.v1.

ANSSI (2015) *National Digital Security Strategy*. Retrieved from https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

APEC (2005) *APEC (Asia-Pacific Economic Cooperation) Cybersecurity Strategy*. Retrieved from https://www.apec.org/docs/default-source/groups/tel/05_tel_apecstrategy.pdf

Argentina Government (2023) *Second National Cybersecurity Strategy*. Retrieved from https://www.argentina.gob.ar/sites / default/files/anexo_6777529_1.pdf

ASEAN (2024) Association of Southeast Asian Nations. https://asean.org/ (accessed 17 November 2024)

Australian Government (2020) *Australia's Cyber Security Strategy*. Retrieved from https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Azmi R, **Tibben W and Win KT** (2018) Review of cybersecurity frameworks: Context and shared concepts. *Journal of Cyber Policy 3*(2), 258–283. https://doi.org/10.1080/23738871.2018.1520271.

Baezner M and Cordey S (2019) *National Cybersecurity Strategies in Comparison – Challenges for Switzerland*. Zürich: Center for Security Studies (CSS)

Barik K, **Misra S**, **Konar K**, **Kaushik M and Ahuja R** (2022) A comparative study on the application of text mining in cybersecurity. *Recent Advances in Computer Science and Communications 16*(3). https://doi.org/10.2174/2666255816666220601113550.

Bechor T and Jung B (2019) Current state and modeling of research topics in cybersecurity and data science. *Systemics, Cybernetics and Informatics 17*(1), 129–156.

Belfer Center for Science and International Affairs (2020) National cyber power ındex 2020 – Methodology and analytical considerations. In *Belfer Center for Science and International Affairs - Harvard Kennedy School* (September), pp. 1–71. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

Blei DM, **Ng AY and Jordan MI** (2003) Latent dirichlet allocation. *Journal of Machine Learning Research*, *3*, 993–1022.

Brasil Presidency of the Republic (2020) *Brasil National Cybersecurity Strategy*. Retrieved from http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Decreto/D10222.htm

Council of Europe (2024) The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols. https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 17 November 2024)

e-Governance Academy (2024) National Cyber Security Index (NCSI). https://ncsi.ega.ee/methodology/ (accessed 16 November 2024)

Enescu S (2020) A comparative study on European cyber security strategies. *Redefining Community in Intercultural Context 9*, 277–282.

ENISA (2012a) *National Cyber Security Strategies*. Retrieved from https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

ENISA (2012b) *National Cyber Security Strategies – Practical Guide on Development and Execution*. Retrieved from https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

ENISA (2014) *An Evaluation Framework for National Cyber Security Strategies European Union Agency for Network and Information Security (ENISA)*. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/e751c1c2-cf11-449c-9fb9-78e5660d49b1/language-en

ENISA (2016) *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies European Union Agency for Network and Information Security (ENISA)*. Retrieved from https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

ENISA (2019) *Good Practices in Innovation Under NCSS European Union Agency for Cybersecurity (ENISA)*. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/3046c9cf-47cb-11ea-b81b-01aa75ed71a1/language-en

ENISA (2020) *National Capabilities Assessment Framework* (Sarri A and Thirriot A (eds.)). The European Union Agency for Cybersecurity (ENISA). Retrieved from https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

ENISA (2024) The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/ (accessed 17 November 2024)

EUI & Booz Allen Hamilton (2011) *Cyber Power Index – Findings and Methodology*. pp. 1–36.

European Commission (2020) *The EU's Cybersecurity Strategy for the Digital Decade*. Retrieved from https://ec.europa.eu/newsroom/dae/redirection/document/72164

European Union (2024) EU General Data Protection Regulation (GDPR). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1731850404866 (accessed 17 November 2024)

Falch M, **Olesen H**, **Skouby KE**, **Tadayoni R and Williams I** (2023) Cybersecurity strategies for SMEs in the Nordic Baltic region. *Journal of Cyber Security and Mobility 11*(6), 727–754.

FIRST (2024) Forum of Incident Response and Security Teams. https://www.first.org/ (accessed 17 November 2024)

German Federal Ministry of Interior (2016) *Cyber Security Strategy for Germany*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en

GFCE (2024) The Global Forum on Cyber Expertise (GFCE). https://thegfce.org/ (accessed 17 November 2024)

Gorka M (2018) The cybersecurity strategy of the visegrad group countries. *Politics in Central Europe 14*(2), 75–98. 10.2478/pce-2018-0010.

Government of Canada (2018) *National Cyber Security Strategy*. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

Government of Mexico (2017) *National Cybersecurity Strategy*. Retrieved from https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf

Ignaczak L, **Goldschmidt G**, **Da Costa CA and Righi RDR** (2022) Text mining in cybersecurity. *ACM Computing Surveys 54*(7), 1–36. 10.1145/3462477.

IISS (2021) *Cyber Capabilities and National Power: A Net Assessment*. Retrieved from https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

Indian Ministry of Communication and IT (2013) *National Cyber Security Policy*. Retrieved from https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

Indonesian Government (2023) *National Cyber Security Strategy*. Retrieved from https://peraturan.bpk.go.id/Download/312229/Perpres%20Nomor%2047%20Tahun%202023.pdf

Iova R and Watashiba T (2023) NCSS: A global census of national positions on conflict, neutrality and cooperation. *European Conference on Cyber Warfare and Security 22*, 420–428. 10.34190/eccws.22.1.1168.

Italian Government (2022) *National Cybersecurity Strategy 2022–2026*. https://www.acn.gov.it/ACN_EN_Strategia.pdf

ITU (2018a) *Guide to Developing a National Cyber Security Strategy – Strategic Engagement in Cybersecurity*. Geneva. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

ITU (2018b) *Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity*. International Telecommunication Union.

ITU (2024) Global Cybersecurity Index (GCI). https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx (accessed 16 November 2024)

Jacuch A (2021) Comparative Analysis of Cybersecurity Strategies. European Union Strategy and Policies. Polish and Selected Countries Strategies. *On-Line Journal Modelling the New Europe 37*(6), 102–120. https://doi.org/10.24193/OJMNE.2021.37.06.

Japanese Government (2021) *Outline of Japan's Next Cybersecurity Strategy*. Retrieved from https://www.nisc.go.jp/eng/pdf/txt_next_CS_strategy_outline.pdf

Kingdom of Saudi Arabia (2020) *National Cybersecurity Strategy*. Retrieved from https://nca.gov.sa/national_cybersecurity_strategy-en.pdf

Kolini F and Janczewski L (2017) *Clustering and Topic Modelling: A New Approach for Analysis of National Cyber Security Strategies*.

Kovacs L (2019) National Cybersecurity Strategy Framework. *Academic and Applied Research in Military and Public Management Science 18*(2), 65–76. https://doi.org/10.32565/aarms.2019.2.9.

Luiijf E, **Besseling K and Graaf P** (2013) Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection 9*, 3. https://doi.org/10.1504/IJCIS.2013.051608.

Montasari R (2023) Cyber threats and the security risks they pose to national security: An assessment of cybersecurity policy in the United Kingdom. In Montasari R (ed.), *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*. Cham: Springer International Publishing, pp. 7–25. https://doi.org/10.1007/978-3-031-21920-7_2.

NATO CCD COE (2012) *National Cyber Security Framework Manual*, Klimburg A (ed.), 1st Edn. NATO CCD COE Publications.

Newmeyer KP (2015) Elements of National Cybersecurity Strategy for Developing Nations. *National Cybersecurity Institute Journal 1*(3), 9–19.

Odebade A and Benkhelifa E (2023) *A Comparative Study of National Cyber Security Strategies of Ten Nations*. https://doi.org/10.48550/arXiv.2303.13938

https://doi.org/10.1017/dap.2024.99 Published online by Cambridge University Press

OECD (2012) *Cybersecurity Policy Making at a Turning Point – Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy Organisation for Economic Co-operation and Development*. Retrieved from http://www.oecd.org/sti/ieconomy/cybersecuritypolicy making.pdf

OpenAI (2024) *OpenAI API*. https://openai.com/blog/openai-api

Organization of American States (2022) *National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions*.

Ovchinnikova O and Upadhyay NK (2023) The level of cybersecurity of the BRICS member countries in ınternational ratings: Prospects for cooperation. *BRICS Law Journal 10*(1), 7–34. https://doi.org/10.21684/2412-2343-2023-10-1-7-34.

Oxford GCSCC (2021) *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Retrieved from https://gcscc.ox.ac.uk/the-cmm

Paris Call (2024) The Paris Call for Trust and Security in Cyberspace. https://pariscall.international/en/ (accessed 17 November 2024)

Potomac Institute for Policy Studies (2015) *Cyber Readiness Index 2.0*. Retrieved from https://potomacinstitute.org/images/CRIndex2.0.pdf

Republic of Turkey (2020) *National Cyber Security Straretgy*. Retrieved from https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/national-cyber-security-strategy-2020-2023.pdf

Russian Federation (2016) *Doctrine of Information Security*. Retrieved from http://kremlin.ru/acts/bank/41460

Sabillon R (2021) *National Cybersecurity Strategies*. pp. 84–102. https://doi.org/10.4018/978-1-7998-4162-3.ch005.

Sabillon R, **Cavaller V and Cano J** (2016) National cyber security strategies: Global trends in cyberspace. *International Journal of Computer Science and Software Engineering 5*(5), 67–81.

Samtani S, **Chinn K**, **Larson C and Chen H** (2016) Azsecure hacker assets portal: Cyber threat intelligence and malware analysis. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. pp. 19–24.

Santisteban AS, **Ocares L and Andrade-Arenas L** (2020) Analysis of National Cybersecurity Strategies. *International Journal of Advanced Computer Science and Applications 11*(12). https://doi.org/10.14569/IJACSA.2020.0111288.

Shafqat N and Masood A (2016) Comparative analysis of various national cybersecurity strategies. *International Journal of Computer Science and Information Security 14*(1), 129–136.

Song M, **Kim DH**, **Bae S and Kim S-J** (2021) Comparative analysis of national cyber security strategies using topic modelling. *International Journal of Advanced Computer Science and Applications 12*(12). https://doi.org/10.14569/IJACSA.2021.0121209.

South Africa State Security Agency (2012) *The National Cybersecurity Policy Framework*. Retrieved from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

South Korea National Security Office (2019) *National Cybersecurity Strategy*. Retrieved from https://ccdcoe.org/uploads/2018/10/South-Korea_English-National-Cybersecurity-Strategy-03-April-2019_English-1.pdf

Štitilis D, **Pakutinskas P and Malinauskaitė I** (2017) EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Security Journal 30*(4), 1151–1168. https://doi.org/10.1057/s41284-016-0083-9.

Sunkph J, **Ramjan S and Ottamakorn C** (2018) Cybersecurity policy in ASEAN countries. In *Information Institute Conferences*. Las Vegas, pp. 1–7. https://www.researchgate.net/profile/Jirapon-Sunkpho-2/publication/324106226_Cybersecurity_Policy_in_ASEAN_Countries/links/5abdc2ea45851584fa6fca37/Cybersecurity-Policy-in-ASEAN-Countries.pdf (accessed 16 November 2024)

The Cyberspace Administration of China (2016) *National Cyberspace Security Strategy*. Retrieved from http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

The White House (2023) *National Cybersecurity Strategy*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Tikk E and Kerttunen M (2020) *Routledge Handbook of International Cybersecurity* (Tikk E and Kerttunen M (eds.)). Routledge. https://doi.org/10.4324/9781351038904.

UK Government (2016) *National Cyber Security Strategy 2016–2021*. Retrieved from https://assets.publishing.service.gov.uk/media/5a81914de5274a2e8ab54ae9/national_cyber_security_strategy_2016.pdf

UNIDIR (2013) *The Cyber Index-International Security Trends and Realities United Nations Publications*. Retrieved from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

United Nations (2024a) *Cyber Security Portal*. https://cyberpolicyportal.org/

United Nations (2024b) United Nations Group of Governmental Experts. https://disarmament.unoda.org/group-of-governmental-experts/ (accessed 17 November 2024)

Wamala F (2011) *ITU National Cybersecurity Strategy Guide*. Retrieved from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

Cite this article: Çifci H and Ergüner E (2025). Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*, 7: e7. doi:10.1017/dap.2024.99