Analysis of Cybersecurity Strategies Across Continents

Pekka Pirinen, Piia Perälä and Martti Lehto
University of Jyväskylä, Finland

pekka.j.pirinen@jyu.fi
piia.m.h.perala@jyu.fi
martti.j.lehto@jyu.fi

Abstract: Cyberthreats are a global challenge and because of that countries across the world have been establishing and developing national cybersecurity strategies (NCSS). NCSSs are a way in which countries can present their political and social approach to cybersecurity in the sense of national security. The main principles of a NCSS are addressing the current cybersecurity landscape that the country in question has, the goals of future national cybersecurity development and how to achieve that desired state of national cybersecurity affairs. Being part of the country's national, political and cultural landscape, the actual cybersecurity strategies naming policies may differ from country to country. Although the most common goals are similar between different states' cybersecurity strategies, they have different emphasis regarding the role of citizens, the private sector and the public sector in national cybersecurity. This study aims to analyze and compare NCSSs from different continents and recognize the focus areas in the three crucial target groups: citizens, private sector and public sector. NCSSs of 20 different countries from Africa, Asia, Europe, North America, Australia and Oceania and South America were analyzed. All the strategies were collected from public sources and represent the latest version of selected countries' cybersecurity strategies. The strategies were analyzed using the Commitment to Development (C2D) approach. The Democracy Index was utilized in the study to recognize and differentiate countries based on their index rating. The main findings of this study were that with a few exceptions countries sharing similar Democracy Index rankings have similar attitudes towards their citizens, private sector and public sector. The results also varied in a continental perspective, and some continents align better with each other than others.

Keywords: Cybersecurity strategy, Comparative analysis, Commitment to development, Citizens, Private sector, Public sector

1. Introduction

Cybersecurity in the national context has become a subject of interest to different countries from all around the world. Countries have started to build their own approach to national cybersecurity. These different national cybersecurity strategies (NCSSs) form a possibility to investigate the countries' strategic national ways of cybersecurity thinking. NCSSs are a part of the countries' national, political and cultural landscape and have different emphasis from country to country.

Previous research on NCSSs has approached the topic from various perspectives. For example, Kleiner (2025) focused on how different political systems influence national cybersecurity. While Carr (2016) analyzed the role of cooperation between the public and private sectors in NCSSs. In addition, NCSSs have been studied to gain understanding for the further development of strategies (e.g., Odebade & Benkhelifa, 2023; Shafqat & Masood, 2016).

Previous research has often focused on a single issue or perspective, such as governmental aspects (e.g., Odebade & Benkhelifa, 2023) or has been limited to specific geographic regions (e.g., Lehto, 2013). This study aims to provide a broader understanding of how countries emphasize different focus areas in their NCSSs. It differs from earlier work by examining how public-private partnership collaboration mechanisms are reflected in NCSSs and how the dimensions of the C2D approach are represented. Furthermore, the study includes strategies from countries across all continents, rather than being limited to one or a few regions.

In this study NCSSs from all the world's continents are analyzed and compared. The strategies are then evaluated by the three focus areas: citizens private sector and public sector. These three focus areas were then divided into different sub focus areas to enhance the analysis.

2. Public-Private Partnership Collaboration Mechanisms

Public-private partnership in cybersecurity can be seen as different ends and means in which governmental public sector collaborates with private sector thus enhancing the different aspects of cybersecurity in the country. The most crucial part of public-private partnership is the protection of cyber-related critical infrastructure, that is operated in one way or another by the private sector in every country of the world. Public-private partnerships collaboration mechanisms have their roots in the 1990's when countries started to privatize their national critical infrastructure for economic development (Carr, 2016).

Public-private partnerships collaboration mechanisms are visible in this study's NCSSs, and they range from economical and educational collaboration to protecting of critical infrastructure and national armed defense. In all the NCSSs some form of public-private partnerships could be observed that would concern the critical infrastructure or national economy.

3. The Commitment to Development (C2D) Approach

Commitment to Development (C2D) is an approach that focuses on cybersecurity from societal and economical point of view by combining different values into cybersecurity policies. The C2D enables countries to identify and act on different national needs and co-operation possibilities and works as a tool for understanding the cybersecurity field and its different aspects in national and international context (Kerttunen & Tikk, 2019).

The C2D consists of three different elements which are direction, strategic capacity and policy analysis. The direction element of C2D focuses on the societal values and political values behind the NCSSs and how the strategies represent them. Strategic capacity is a set of different aspects in the NCSSs that enhance the national capabilities offering sustainable security to the country. Policy analysis focuses on how the different NCSSs policies are defined into measurable metrics. (Kerttunen & Tikk, 2019.)

In the previous research, the C2D approach has been utilized by Busetti and Scanni (2025) where the C2D was used to analyze the national security role of securing critical infrastructure in cyberspace.

4. Methodology

The study material consists of NCSSs from 20 different countries across every continent. The strategies were selected in a way that at least three countries were included from each continent. The selection of countries was based on the Democracy Index, ensuring that within each continent, the chosen countries represented varying levels of democracy. The Democracy Index ranks countries in the scale of 1 being an authoritarian country to 10 being a full democracy. By utilizing the Democracy Index in the study, it is possible to investigate how the countries in different democracy levels view cybersecurity and how the different areas (citizens, private sector & public sector) contribute to cybersecurity. Table 1 presents the countries included in the study along with their Democracy Index rankings and the publication years of their NCSSs and the publisher of the strategy.

Table 1: Continents, countries, their 2024 Democracy Index rating and the publisher of the strategy.

Continent	Country	Democracy Index 2024	Year of Strategy Publication	Publisher
Asia	Saudi Arabia	2,08	2020	Kingdom of Saudi Arabia
Africa	Eswatini	2,6	2022	Eswatini Communications Commission
Asia	Pakistan	2,84	2021	Government of Pakistan
Africa	Tanzania	5,2	2022	President´s Office & Public Service Management and Good Governance
North America	Mexico	5,32	2017	Government of Mexico
South America	Paraguay	5,92	2025	Government of Paraguay
Australia & Oceania	Papua New Guinea	5,97	2024	The Independent State of Papua New Guinea
Europe	Romania	5,99	2022	Government of Romania
South America	Argentina	6,51	2024	Republic of Argentina National Executive Branch

Continent	Country	Democracy Index 2024	Year of Strategy Publication	Publisher
Asia	India	7,29	2020	Data Security Council of India
Africa	Botswana	7,63		Ministry of Transport and Communications
Europe	Latvia	7,66	2023	Ministry of Defense
Asia	Israel	7,8	2025	Israel National Cyber Directorate
North America	USA	7,85	2023	The White House
Asia	Japan	8,48	2021	The Government of Japan
South America	Uruguay	8,67	2024	The President of Uruguay
North America	Canada	8,69	2025	Ministers of Public Safety and Emergency Preparedness
Australia & Oceania	Australia	8,85	2023	Australian Government
Europe	Finland	9,3	2024	Prime Minister´s Office
Australia & Oceania	New Zealand	9,61	2019	New Zealand Government

Content analysis by Weber (1990) was used to identify the content of the strategies. Atlas.ti software was used for the analysis. The strategies were uploaded to Atlas.ti and coding was made based on the three different focus areas and their sub areas. For the analysis, the C2D approach was utilized. The analysis was conducted in three phases.

In the first phase, the strategies were examined to identify how the public-private partnership collaboration mechanism is manifested at the strategic level. The analysis focused on how citizens, the private sector, and the public sector are represented in NCSSs. For example, the roles that these different actors play in national cybersecurity.

In the second phase, the public-private partnership was analyzed in the context of the countries' Democracy Index rating. After that the NCSSs were compared within and between continents.

In the third phase, the public-private partnership was analyzed in more depth to understand how the dimensions of the C2D approach and most specifically its direction aspect was reflected in this collaboration mechanism.

5. Research Results

5.1 Citizens

Four sub focus areas were utilized to differentiate the countries' emphasis on citizens between each other. The sub focus areas are how the NCSSs consider *the citizens in legislation* (legislation affecting citizens), *the individual citizens' rights* (mentions about citizens' rights), *citizen agency* (mentions of citizens agency) and *the safety and privacy of citizens* (mentions about citizens safety or privacy).

Asian countries varied from each other. Pakistan does not view its citizens as an active agency and emphasizes the importance of securing the cyberspace of its citizens (Government of Pakistan, 2021). India has also a similar security first perspective to its citizens in the cyberspace. The focus of India´s strategy considering its citizens is to secure the country´s cyber infrastructure for its citizens in the normal and emergency conditions (Data Security Council of India, 2020).

Saudi Arabia has a business-oriented attitude on its citizens. All the citizens' agencies are based on their business attributes (Kingdom of Saudi Arabia, 2020). Israel emphasizes that the citizens of Israel are active participants in

the cyberspace and regarding the national security of the country every citizen has a duty to protect the nation in emergency situations. Israel also brings up the role of democracy regarding its citizens. (Israel National Cyber Directorate, 2025.) Japan emphasizes that its citizens as active agency should have the opportunity to participate in a democratic and rights-respecting protected cyberspace. Japan sees its citizens as a crucial factor in building the country´s secure cyberspace. (The Government of Japan, 2021.)

The European countries Finland, Latvia and Romania have very similar relation to their citizens role in their NCSSs. Latvia sees its citizens as agency that have clear roles in national cybersecurity in the case of national emergency. Latvia also emphasizes that citizens' rights should be protected in all circumstances. (Ministry of Defense, 2023.) Finland also sees its citizens as a crucial part of the whole society as a cybersecurity provider and emphasizes the citizens role and responsibility in the civilian defense of the national cyberspace. Finland also emphasizes that the government should ultimately guarantee the citizens' rights and security in the cyberspace. (Prime Minister´s Office, 2024.) Romania sees its citizens as active agency and emphasizes that every Romanian citizen has a role in the national cyber defense. Romania also emphasizes that every citizen should be responsible for their actions in the cyberspace. (Government of Romania, 2022.)

The countries in the Australia and Oceania have similarities and differences in their emphasis on their citizens roles in cybersecurity. Australia views its citizens as agency but emphasizes that the government should have a stronger role in protecting their citizens and their rights in the cyberspace (Australian Government, 2023). Papua New Guinea emphasizes that the rights and security of its citizens in the cyberspace should be protected, and citizens need to assist the government in securing the cyberspace. Papua New Guinea also emphasizes that the level of its citizens cybersecurity skills should be improved to improve the country´s national cybersecurity situation. (The Independent State of Papua New Guinea, 2024.) New Zealand emphasizes that the individual citizen is an agency and a cybersecurity provider to the country. New Zealand also emphasizes the citizens' rights and states that the country needs the contribution of its citizens to secure the national cyberspace. (New Zealand Government, 2019.)

The South American countries have an emphasis on focusing to protect the rights of their citizens in the cyberspace. Argentina emphasizes that the citizens privacy and rights need to be secured but does not view an individual citizen as a major agency and emphasizes the government´s role in building secure national cyberspace (Republic of Argentina National Executive Branch, 2024). Uruguay emphasizes that citizens are a crucial part of building the strategy and one of the objectives is to secure the citizens' rights and privacy in the national cyberspace. Uruguay also emphasizes that the citizens should also have responsibility for their own actions in the cyberspace. (The President of Uruguay, 2024.) Paraguay emphasizes need of citizens participation in the planning of the countries cyber policies. Paraguay also acknowledges that the country´s current legislation is not efficient enough to protect the citizens' rights and privacy in the cyberspace. (Government of Paraguay, 2025.)

In Northern American countries, there were major similarities between USA and Canada. Mexico has differences in its focus on its citizens. USA emphasizes that its citizens have too great responsibility for protecting the national cybersecurity and that the government should do more to protect the citizens in cyberspace. USA also highlights the role of co-operation between the citizens, and government to tackle cybersecurity issues. (The White House, 2023.) Canada also emphasizes that citizens have a too great role and responsibility in national cybersecurity. Canada sees cybersecurity as a whole society project and citizens as agency can do their part in protecting their own actions in the cyberspace. (Ministers of Public Safety and Emergency Preparedness, 2025.) Mexico emphasizes in its strategy that the government should protect the citizens' rights and privacy in the cyberspace and that citizens were involved in the making of the strategy. Mexico also acknowledges that the cyber maturity level of its citizens is not yet as high as it should be. (Government of Mexico, 2017.)

The countries in Africa have also similarities and differences in their attitudes towards their citizens. Botswana sees that the national cybersecurity is a whole society project, and its citizens are an agency and that the government's responsibility is to ensure an open and protected cyberspace for its citizens (Ministry of Transport and Communications, 2018). Tanzania recognizes that the country´s and its citizens cyber maturity level is low and that the citizens of the country are in a need of trustworthy cybersecurity infrastructure. The citizens of Tanzania are seen as a beneficiary of the strategy. (President´s Office & Public Service Management and Good Governance, 2022.) Eswatini also recognizes the low level of the country's citizens cyber maturity but also emphasizes that the citizens are responsible for producing national cybersecurity on their part (Eswatini Communications Commission, 2022).

5.2 Public Sector in the Role of National Defense and Armed Forces

The role of public sector regarding the countries' cyber defense was also one of the sub focus areas that were evaluated in the NCSSs. The role of public sector in cyber defense area differed between countries.

Asian countries have different attitudes regarding public sector and its role in national cyber defense. India and Saudi Arabia emphasize means of public civil defense in their NCSSs (Kingdom of Saudi Arabia, 2020; Data Security Council of India, 2020). Pakistan emphasizes in its strategy that the country´s Mil-CERT-teams should contribute to the security of public sector (Government of Pakistan, 2021). The two countries that stand out in Asia are Japan and Israel. Japan emphasizes that a cyberattack against Japan could be compared to an armed attack and the armed forces is ready to defend Japan (The Government of Japan, 2021). Israel emphasizes that the whole public sector works as a part of national defense with the armed forces and the country is willing to proactively act against cyber domain adversaries (Israel National Cyber Directorate, 2025).

European countries view the role of public sector and armed forces similarly. Romania emphasizes that the country´s national cyber defense should be based on NATO standards (Government of Romania, 2022). Finland and Latvia have more comprehensive approach. Finland emphasis that cyber defense is way to secure the operating conditions of the armed forces and recognizes that the whole society´s cyber defense can´t be under the responsibility of the armed forces (Prime Minister´s Office, 2024). Latvia emphasizes that in the case of emergency the armed forces would protect the society (Ministry of Defense, 2023).

Countries in Australia and Oceania also had different views regarding the role of public sector in the national cyber defense. New Zealand does not have a defensive perspective in its strategy. Australia only emphasizes the civilian defense role of its public sector (Australian Government, 2023). Papua New Guinea has the only military dimension regarding its public sector describing that the country´s Defence Cyber Intelligence Unit protects the country´s sovereignty in cyberspace (The Independent State of Papua New Guinea, 2024).

South America has a very similar way of viewing the role of public sector in the cyber defense area. In Argentina the role of the country´s armed forces is to protect country´s national cyberspace (Republic of Argentina National Executive Branch, 2024). Uruguay and Paraguay both emphasize that their armed forces protect their national cyberspace but also need to upgrade their cyberoperation capabilities to protect their sovereignty (The President of Uruguay, 2024; Government of Paraguay, 2025).

Canada and USA in North America have a similar way of viewing the role of public sector providing cybersecurity in the national level. USA emphasizes that the DoD if needed can pre-emptily disturb and neutralize cyberthreats (The White House, 2023). Canada also emphasizes that the armed forces jointly engages in operations that ensure the country´s safety in cyberspace (Ministers of Public Safety and Emergency Preparedness, 2025). Mexico sees the role of public sector in cyber defense as protecting the nations critical infrastructure (Government of Mexico, 2017).

African countries also differ in their attitudes towards public sector role in cyber defense. Tanzania does not have a cyber defensive perspective. Botswana emphasizes that the MoD is responsible for the country´s national cybersecurity (Ministry of Transport and Communications, 2018). Eswatini emphasizes that the country´s armed forces protect the country´s national cyberspace by cyberwarfare is necessary (Eswatini Communications Commission, 2022).

5.3 Private Sector

Five different sub focus areas were utilized to differentiate the countries between each other. The sub focus areas are *private sector´s role in national defense*, *private sector under state guidance*, *private sector in co-operation with the state*, *private sector´s security* and *private sector´s liability*.

Countries in Asia have differences and similarities towards the role of private sector. Pakistan emphasizes that the state should guide the private sector in favor of the national and the private sector´s security (Government of Pakistan, 2021). India and Saudi Arabia have a business-oriented perspective to private sector, but they also emphasize on strong state lead (Kingdom of Saudi Arabia, 2020; Data Security Council of India, 2020). Japan and Israel view that private sector and the state need to work in co-operation to protect the national security and economy (The Government of Japan, 2021; Israel National Cyber Directorate, 2025).

The European countries Finland, Latvia, and Romania have a similar perspective on private sector. Finland emphasizes the voluntary co-operation to improve the country's overall cybersecurity and national cyber defense (Prime Minister´s Office, 2024). Romania views the private sectors roles similarly as Finland but also

emphasizes the liability of private sector in national security (Government of Romania, 2022). Latvia also views the roles of private sector similarly emphasizing the private sector's role and liability in the national defense sector (Ministry of Defense, 2023).

Countries in the Australia and Oceania have also differences towards the role of private sector in national cybersecurity. Australia and New Zealand view that the private sectors focus is on the cybersecurity markets and in strong voluntary co-operation (Australian Government, 2023; New Zealand Government, 2019). Papua New Guinea views the role of the private sector being under the state´s guidance in building and developing the country´s cyber capabilities (The Independent State of Papua New Guinea, 2024).

The South American countries Argentina, Paraguay & Uruguay have a very similar attitude towards the role of private sector in national cybersecurity landscape. All the countries emphasize the voluntary co-operation aspect focusing on the economic aspects of this co-operation (Republic of Argentina National Executive Branch, 2024; The President of Uruguay, 2024; Government of Paraguay, 2025).

In North America there are similarities between USA and Canada as Mexico differs in its view of private sectors role in national cybersecurity. USA emphasizes co-operation, and the private sector should have liabilities on national cybersecurity (The White House, 2023). Canada also emphasizes on co-operation but also points out that the state can guide the private sector if necessary (Ministers of Public Safety and Emergency Preparedness, 2025). Mexico emphasizes that the private sector needs the guidance of the state to improve their cyber capabilities (Government of Mexico, 2017).

The African countries have also different viewpoints into the role of private sector in national cybersecurity. Tanzania emphasizes that the country´s cyberspace resorts to private sector and Botswana emphasizes the role of voluntary co-operation in building the country´s cyber capabilities (President´s Office & Public Service Management and Good Governance, 2022; Ministry of Transport and Communications, 2018). Eswatini emphasizes that private sector needs to be guided by the state to accomplish a secure private sector and national cyberspace (Eswatini Communications Commission, 2022).

6. C2D Capacity and the Different Sectors

While evaluating the role of three focus areas through the C2D approach and specifically its direction section, it can be indicated that the countries and their strategies follow the framing that C2D approach sets. According to the direction section of C2D it´s essential to countries that their cybersecurity thinking should be based on their nations' fundamental base values and national development policies (Kerttunen & Tikk, 2019). The countries emphasized their own national fundamental values which ranged from economic growth and individual rights to national defense and democracy. Every country differs from each other, and the evaluated strategies had strong indications of the country's direction regarding their national cybersecurity.

7. Key Themes and Research Findings

When reviewing the roles that countries give to their citizens there are clear differences and similarities between the countries based on their DI ranking. Highly ranked countries like New Zealand and Finland emphasize that their citizens are an active agency and countries with a lower DI ranking like Pakistan and Saudi Arabia emphasize that their citizens are not as strong agency and more control and protection from the state is needed.

If we look at the countries emphasis on their citizens' role from continental viewpoint, there are similarly aligned and differing continents. European countries emphasize their citizens´ role in building and securing their national cyberspace. South American countries emphasize on their citizens' rights and privacy in cyberspace. In North America, Canada and the USA have a similar attitude towards their citizens where as Mexico´s attitude towards its citizens is similar the South American countries. African countries common factor is that citizens are a developing and increasingly stronger part of the national cybersecurity. Australian and Oceanian countries emphasize that, if necessary, the state will protect the citizens in cyberspace respecting their rights. Asian Israel and Japan have a similar emphasis on their citizens viewing them as strong agency while promoting the role of rights and democracy. Other Asian countries India, Pakistan, and Saudi Arabia focus on their citizens role as being not as a strong agency focusing the citizens security and role in the national economy.

When reviewing the role of public sector in national cyber defense and armed forces, the DI ranking does not reflect into the countries' emphasis on the matter. Highly ranking countries like Finland and Australia do not share a similar view of public sector in armed cyber defense and lower ranking countries like Pakistan and Eswatini have similarities in their view of public sectors role in armed cyber defense.

The continents can be divided into similarly aligning and differentiating. South American countries similarly view the role of public sector in the cyber defense and their armed forces in the cyberspace. The European countries also have a similar basis on their public sectors' role in the cyber defense area. In North America, the USA and Canada have similar emphasis on the public sectors role as Mexico differs from the two. In Australia and Oceania, Australia and New Zealand do not emphasize the armed side of public sector whereas Papua New Guinea acknowledges it. Countries in Africa also fall into two categories where Tanzania does not recognize the armed side and Eswatini and Botswana have mentioned the armed side of public sector in cyberspace. The Asian countries have the most variance. India and Saudi Arabia do not discuss the armed side of public sector. Pakistan, Israel, and Japan all discuss the public sector's role in armed cyber defense.

The role of private sector does align with the DI rankings with some exceptions. Countries with a higher DI ranking like Australia and the USA emphasize the meaning of co-operation with the private sector in cybersecurity whereas lower ranking countries like Eswatini and Saudi Arabia emphasize the role of state lead private sector in cybersecurity.

The continents share similar differences and similarities in the role of private sector as previously have been discussed. In Africa Botswana and Tanzania emphasize more on voluntary co-operation whereas Eswatini emphasized the role of state lead and security. In Australia and Oceania, the countries focus on security side of private sector and Australia and New Zealand emphasize the voluntary co-operation whereas Papua New Guinea focuses on more developing the country´s private sector under state guidance. The European countries have a very similar perspective on private sector and its role in national cybersecurity emphasizing the role of voluntary co-operation. The South American countries also emphasize the role of voluntary co-operation. In North America Mexico differs from the USA and Canada by emphasizing the role of state lead in developing the country´s cyber capabilities, whereas the USA and Canada focus more on voluntary co-operation.

When observing the NCSSs through the C2D approach and its direction section one can argue that the different countries' base national values and policies are visible in all the three observed focus areas. Countries that resemble each other in their political and ideological values emphasized similar attributes regarding the focus areas. For example, when looking through the continental viewpoint all the European countries have similar attitudes in all the three focus areas.

When looking at the countries through their DI rating it can be argued that the countries sharing similar DI ranking also have similar attitudes towards the three focus areas. Highly functioning democracies share similar attitudes and countries with a more authoritative system have similar attitudes towards focus areas. All of this is based on their direction, and it shows clearly.

8. Implications and Future Research

Alignment between the countries' DI ranking and their relation to their national cybersecurity can be observed in two of the three focus areas. In the role of citizens and private sector there can be seen a connection between the DI ranking and the strategies C2D direction. However, there could be other reasons for the connection that this study does not investigate as thoroughly like the European countries having alliances in the EU and NATO.

When comparing this study to the previous research, similar and differing results can be seen. What differs this study is the utilization of Democracy Index ranking and the C2D approaches direction aspect and the combination of civil national cybersecurity into the armed side of national cybersecurity.

Possible future research toward this style of cybersecurity study could have a larger proportion of countries and possibly also take advantage of the older versions of their NCSSs creating a continuum to more strongly understand the direction behind their different focus areas.

AI declaration: No AI was used in this study.

Ethics declaration: No ethical clearance was needed for this study.

References

Australian Government. (2023) *2023–2030 Australian Cyber Security Strategy*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Busetti, S. & Scanni, F.M. (2025*) Evaluating cybersecurity strategies in the energy sector. Evidence from Italy.* Rivista di Digital Politics, 1, pp.165–194. https://doi.org/10.53227/117428

Carr, M. (2016) '*Public–private partnerships in national cyber-security strategies*', International Affairs, 92(1), pp.43–62. doi:10.1111/1468-2346.12504.

Data Security Council of India. (2020) *National Cyber Security Strategy 2020.* https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf
Eswatini Communications Commission. (2022) *Eswatini National Cybersecurity Strategy 2022-2027* https://www.esccom.org.sz/publications/reports/docs/Eswatini_National_Cybersecurity_Strategy_2022-2027.pdf
Government of Mexico. (2017) *National Cybersecurity Strategy*. https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf
Government of Pakistan. (2021) *National Cyber Security Policy 2021*. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf
Government of Paraguay. (2025) *Estrategia Nacional de Ciberseguridad 2025–2028*. https://mitic.gov.py/eoj0cad9uplo/2025/05/ENC-Paraguay-2025-2028-Mayo-20251558.pdf
Government of Romania. (2022) *Strategiei de securitate cibernetică a României, pentru perioada 2022–2027*. https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf
Israel National Cyber Directorate. (2025) *Israel National Cyber Security Strategy 2025*. https://www.gov.il/BlobFolder/news/cyber_strategy_2025/en/israel_national_cybersecurity_strategy_feb2025.pdf
Kerttunen, M. & Tikk, E. (2019) *National Cyber Security Strategies: Commitment to Development,* Cyber Policy Institute, 1, pp. 1–14.
Kingdom of Saudi Arabia. (2020) *National Cybersecurity Strategy*. https://nca.gov.sa/national_cybersecurity_strategy-en.pdf
Kleiner, J. (2025) '*How political regimes affect national cybersecurity: the polity flux effect'*, Democratization, 32(5), pp. 1181–1212. doi: 10.1080/13510347.2025.2451951.
Lehto, M. (2013) *The Ways, Means and Ends in Cyber Security Strategies.* In: Proceedings of the 12th European Conference on Information Warfare and Security, pp.182–190.
Ministers of Public Safety and Emergency Preparedness. (2025) *Canada's National Cyber Security Strategy: Securing Canada's Digital Future*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/ntnl-cbr-scrt-strtg-2025-en.pdf
Ministry of Defense. (2023) *The Cybersecurity Strategy of Latvia 2023–2026*. https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf
Ministry of Transport and Communications. (2018) *National Cybersecurity Strategy*. https://www.bocra.org.bw/sites/default/files/documents/approved%20botswana-national-cybersecurity-strategy.pdf
New Zealand Government. (2019) *New Zealand's Cyber Security Strategy 2019: Enabling New Zealand to Thrive Online*. https://www.dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf
Odebade, A.T. & Benkhelifa, E. (2023) *A comparative study of national cyber security strategies of ten nations*. *arXiv preprint* arXiv:2303.13938.
Prime Minister's Office. (2024) *Finland's Cyber Security Strategy 2024–2035*. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf?sequence=1&isAllowed=y
Republic of Argentina National Executive Branch. (2023) *Estrategia Nacional de Ciberseguridad de la República Argentina*. https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904
Shafqat, N., & Masood, A. (2016) *Comparative analysis of various national cyber security strategies.* International Journal of Computer Science and Information Security, 14(1), 129-136.
The Government of Japan. (2021) *Cybersecurity Strategy*. https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf
The Independent State of Papua New Guinea. (2024) *National Cyber Security Strategy*. https://www.ict.gov.pg/wp-content/uploads/2024/policies/Final%20PNG%20NCSS-%20rev%2004-04-24.pdf
The President of Uruguay. (2024) *Estrategia Nacional de Ciberseguridad del Uruguay 2024–2030*. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/book/8671/download
President´s Office & Public Service Management and Good Governance. (2022) *Government Cybersecurity Strategy 2022.* https://www.utumishi.go.tz/uploads/documents/sw-1697717419-GOVERNMENT%20CYBER%20SECURITY%20STRATEGY%202022.pdf
The White House. (2023) *National Cybersecurity Strategy*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
Weber, R. P. (1990) *Basic Content Analysis*. SAGE Publications, Inc.