National Cybersecurity Strategies:

Lessons Learned and Reflections from the Americas and Other Regions

OAS More rights for more people

GLOBAL PARTNERS DIGITAL

TABLE OF **CONTENTS**

ACKNOWLEDGMENTS

Luis Almagro
Secretary General of the Organization of American States (OAS)

Lea Kaspar
Executive Director, Global Partners Digital

OAS Technical Team
Arthur Weintraub
Alison August Treppel
Kerry-Ann Barrett
Sofía Hunter
David Moreno
Mariana Jaramillo

GPD Technical Team
Daniela Schnidrig
Ruby Khela

Contributors
Cynthia Wright, The MITRE Corporation
Ian Ralby, Consultant
Derechos Digitales
Fundación Karisma
Governments of Colombia, Mexico and Uruguay

The development of this document was made possible with support from the Ministry of Foreign Affairs of the Netherlands and Global Affairs Canada.

ABOUT THE **AUTHORS**

The **Organization of American States (OAS)** was established in 1948 through the Charter of the OAS in order to achieve among its member states—as stipulated in Article 1 of the Charter—"an order of peace and justice, to promote their solidarity, to strengthen their collaboration, and to defend their sovereignty, their territorial integrity, and their independence." Bringing together all 35 independent states of the Americas, the OAS uses a four-pronged approach to effectively implement its essential purposes, based on its main pillars: democracy, human rights, security, and development. The OAS/CICTE Cybersecurity Program has been working for over a decade to strengthen cybersecurity capabilities in OAS Member States based on a multi-pronged multi-stakeholder engagement approach.

With over 16 years of experience, CICTE's Cybersecurity Program has become a regional leader in assisting countries in Latin America and the Caribbean (LAC) to build technical and policy-level cybersecurity capacity. The initiatives and activities carried out by the Program aim at ensuring an open, secure and resilient cyberspace throughout the Western Hemisphere. In an age of steadily increasing Internet connectivity, countries' socioeconomic progress directly relies on a secure and reliable cyberspace that allows for the free flow of information and economic transactions. The OAS was the first regional body to adopt a regional cybersecurity framework (2004), which addressed key areas such as public awareness, public-private partnerships, and capacity-building. The Cybersecurity Program's approach in this area consists in facilitating the organization of national roundtable discussions with the participation of key national cybersecurity stakeholders, including government representatives, private sector, civil society, and academia. Facilitated by OAS experts, sessions first seek to familiarize participants with the purpose of national cybersecurity strategies, and to introduce them to the function and components of a number of strategies that are in effect around the world.

Global Partners Digital (GPD) is a non-governmental organization working to enable a digital environment underpinned by human rights. GPD has been implementing a cyber capacity-building portfolio for over 8 years, aimed at making cybersecurity discussions more open, inclusive, and transparent, as well as making policy outcomes human rights respecting through a four-pronged approach: undertaking monitoring and analysis of trends, building stakeholder capacity, fostering alliances, and coordinating action, and direct advocacy.

GPD currently works in over 15 countries in Latin America, Sub-Saharan Africa, and Asia Pacific, where it supports civil society partners to build their capacity on cyber policy issues and engage in cybersecurity policymaking and implementation processes to bring human rights considerations to those discussions.

INTRODUCTION

When there is trust in our online environment, businesses and governments can operate safely, and individuals can exercise their rights and enjoy the freedom that digital technology affords. This growing interconnectedness between society, technology, and the economy has caused governments to consider how to protect their citizens and critical infrastructure from threats in the digital environment. As such, the existence of a free, open, and secure cyberspace is intrinsically linked to social and economic development.

The prevalence, diversity, complexity, and severity of existing and emerging cyber threats require a shift from reactive ad-hoc responses to a more structured, cohesive, and strategic approach to addressing cyber threats in a manner that respects human rights. As a result, governments are increasingly turning to the development of National Cybersecurity Strategies (NCS) to address a broad range of issues at the policy level, providing a strategic pathway and framework to doing so in a sustainable way. It is important at this juncture to acknowledge that while the NCS cannot address a government's digital agenda in its entirety (for example the considerations around government digital migration and national connectivity programs), it stands as a good interlocutory for those initiatives and considers security by design.

From our experience working in the Americas, it has become evident that developing a strategic approach to addressing cyber threats is no easy task. NCSs in the region are beginning to be seen as key instruments to address cyber threats and build resilience. In this effort, countries have grappled with finding the right approach to developing and implementing an NCS.

The authors of this paper aim to address this challenge by offering information on the possible approaches to policymakers working on the development, implementation, and review of NCSs in the Americas. We include descriptions of different possible approaches and considerations, illustrated through examples from some OAS member states and other globally relevant resources, for developing an NCS and addressing cybersecurity threats. Developing and implementing an NCS is a mammoth task, but assessment tools and guides are available to support a holistic and sustainable effort.

While policymakers responsible for the development, implementation, and review of NCSs in the Americas are the primary audience of this resource, we hope that this document will also be a helpful resource for any stakeholder working in the field of cybersecurity capacity-building. By providing practical examples of good practice, the document can inform the design and delivery of projects focused on NCS and can otherwise be used at any point in the NCS development, implementation, or review process. In addition to this, the authors hope that the document will be a useful resource to inform international peace and security discussions, where NCSs are seen as key instruments to advance cybersecurity capacity building and contribute to the implementation of agreed norms and confidence building measures for responsible State behavior in cyberspace.

Approach and document structure

This document is structured in five parts that address the key considerations relevant for the process of NCS development, implementation, and review.

Part One makes a case for prioritizing the development of an NCS as it describes some of the challenges in cybersecurity today, both at the national and international levels. It also considers the role an NCS plays in supporting societal and economic developmental goals.

Part Two focuses on the need to follow a multistakeholder approach to developing an NCS. Multistakeholder efforts

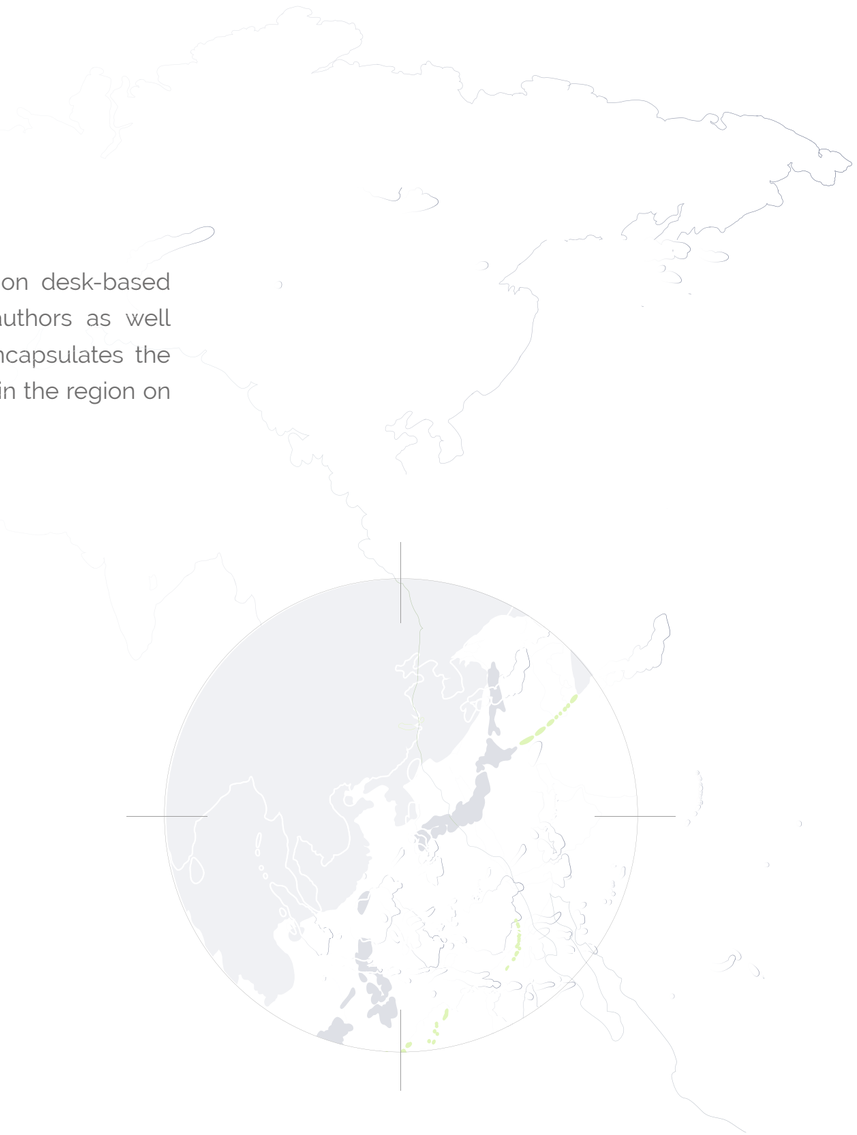
provide value by bringing in multiple viewpoints and easing the road to general buy-in and support with the implementation of the NCS.

Part Three offers descriptions in a neutral, agnostic (i.e., "tool-nostic" and "guide-nostic") way for several existing assessment tools and guides, including information on applicable regional and global programs. While none of these should be used straight "out of the box", they may serve as an excellent starting point to help determine where a nation is in its cyber capacity and how it might best move forward.

Part Four moves from the general considerations of tools and guides into practical approaches around implementing an NCS, including bringing together multistakeholder committees, prioritizing the goals and objectives, and considering the monitoring and evaluation process that is so critical to the success of an NCS.

Part Five provides several case studies comparing NCS development and implementation in several countries and regions in the Americas. Included in this section is a sectoral case study focusing on how cybersecurity in the maritime sector aligns with the needs and processes of an NCS.

The development of the document is built on desk-based research by the authors and contributing authors as well as interviews with OAS member states; it encapsulates the experiences of the work of the OAS and GPD in the region on this topic.



Part **1**

ADVOCATING FOR A NATIONAL **CYBERSECURITY STRATEGY**

The first half of Part One focuses on key considerations for countries to consider when defining the need for an NCS, such as how robust cybersecurity frameworks promote sustainable development and the exercise of human rights, and how they are key to addressing cyber threats. The second half provides examples of different types of motivation behind starting a process of developing an NCS, focusing on the driving factors that lead to a nation concluding it needs to formalize its NCS. These factors may include the need to promote sustainable development, the experience of a cyberattack, receipt of a digital investment loan, or the desire to promote digital transformation, among other possible reasons.

CYBERSECURITY CHALLENGES TODAY

With the increase in Internet usage, the dividing line between the real world and the digital world is rapidly fading. Improved efficiency and productivity because of technological advancement are also unparalleled, and people's dependence on technology has been further heightened by major global events.[1] Strong cybersecurity can lead to an online environment that enables and empowers individuals to exercise their rights and enjoy their freedoms and is a prerequisite for user trust. User trust, in turn, is crucial for sustained uptake and use of the Internet. The absence of strong cybersecurity and user trust is an obstacle to meaningful access and the future growth of the digital economy.[2]

Unfortunately, the growth rate of the Internet has outpaced cybersecurity capacity, lowering the barriers of entry, both in terms of availability and accessibility, for illicit activities. With such low barriers of entry, cybercriminals are flooding the market. Crimes can be committed from any remote location, and criminals no longer need to worry about law enforcement agencies in the country where they are committing crimes. Criminals are even more innovative in adopting existing tools to become more pervasive across the Internet. Crimes in the "real" world are now more closely linked to the digital world, which makes us wonder if it is still correct to continue distinguishing between a "real" vs. "digital" world. The border between real and digital is very thin and many people and infrastructures have become victims of hacking, theft, identity theft, and malicious software. While law enforcement agencies and governments attempt to tackle this problem, the rate of cybercrime continues to grow, law enforcement's ability to link the crime to the author and jurisdiction is declining and it's becoming imperative for policymakers to build their expertise on cybersecurity and technology issues more broadly. Paradoxically, the same systems that make it easier for people to conduct e-commerce and online transactions are the same cybercriminals are exploiting.

On the positive side, governments and business leaders are more aware than ever that the gains to be had from digital connectivity must be balanced by the need to manage cybersecurity risks and resilience in the face of cyber threats. Planning for these types of issues has become a permanent topic for risk management for governments and other stakeholders. As the number and complexity of attacks grow, the resources available to combat these attacks, such as frameworks, guidelines, information sharing efforts, capacity-building programs, and commercial services related to cyber risk management, also grow.

SOCIETY AND CYBERSECURITY

As we all know, the Internet has been characterized as borderless and a platform through which we all can speak. Through this medium, many people have been able to access services and basic human needs such as education and medical appointments that were not readily available or affordable before. In a 2011 report titled *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, former UN Special Rapporteur Frank La Rue acknowledges that the Internet has become such a fundamental tool for asserting other human rights that people must not be denied its use. He was quoted as saying,

> "Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all states."[3]

Furthermore, the United Nations Sustainable Development Goals (SDGs, also known as the Global Goals) were adopted by all United Nations Member States in 2015 as a universal call to action to end poverty, protect the planet, and ensure that all people enjoy peace and prosperity by 2030.[4] Among the 17 SDGs is Goal 9, which among its targets aims to significantly increase access to Information and Communications Technology (ICT) and strive to provide universal and affordable access to the Internet in the least developed countries. Goal 9 recognizes the existing digital divide, given that only a percentage of the world's population currently has access to the Internet, leaving an estimated 3.6 billion disconnected.[5] This gap makes digital inclusion a key priority for governments and international organizations.[6] From government to small towns, knowledge and information opens a whole world of opportunities. It guides what people do and the way they do it. The UN 2030 Agenda recognizes the need to develop knowledge societies where everyone has opportunities to learn and engage with others and highlights the need for access to ICTs.[7]

As much of the work to achieve these outcomes relies on ICT, the Internet is key to helping in the implementation and monitoring of the SDGs. Although promoting greater access to the Internet is essential, the role of digital technologies in achieving the Global Goals goes far beyond. With the right policies, investments in infrastructure and human capacity, and cooperation among stakeholders, fields as diverse as health and education, governance, economic empowerment and enterprise, agriculture, and environmental sustainability can be revolutionized.

If solely supported by ICTs, this growth is unsustainable if the risks of increased reliance on ICTs are not recognized and managed. Consequently, cybersecurity becomes a key player in achieving these SDGs. According to the report Securing Digital Dividends: Mainstreaming Cybersecurity in International Development by Robert Morgus, without cybersecurity,

> "ICT becomes a potential new point of failure that could threaten to undo development progress. It is therefore compelling that efforts are unified in order to build capacity to manage and confront cyber risks."[8]

If technology is unreliable and untrustworthy, countries and citizens may not take full advantage of the benefits of digitization. Even worse, increased reliance on digital technology, together with unreliability, may actually create negative progress.

Despite global progress in expanding the use of the Internet, the digital gap between developed and developing countries remains wide. A vast part of the world's population remains offline and excluded from the benefits of digitalization, which leads, in some cases, to the governments taking out loans in order to become digital societies. These loans are mainly funded by international organizations such as UNCTAD, the International Telecommunication Union, the United Nations Industrial Development Organization (UNIDO), The World Bank, and others. This gap was further emphasized in 2020 with the onset of the COVID-19 pandemic, which has only heightened humans' technological dependence. The COVID-19 crisis has

accelerated the process for many governments to move online and has become a catalyst for rapid change, bringing new challenges and opportunities. For example, governments have embraced the opportunity to provide information related to the pandemic on national portals, mobile apps, or social media platforms. At the same time, however, the governments face new challenges in the form of disinformation and viral hoaxes as users with bad intentions or insufficient knowledge contribute to the spread of fake news and create further panic in society. As part of the increased reach of the pandemic, thousands of COVID-19 scam and malware sites have emerged daily, such as the sale of counterfeit surgical masks, fake self-testing kits, and so on. In addition, Deloitte reports on how, between February 2020 and May 2020, criminals exploiting cybersecurity weaknesses in remote working platforms impacted over half a million people through the theft and subsequent sale of their personal information (e.g., name, passwords, email addresses).[9]

The reality is that new challenges will continue appearing every day, and COVID-19 will – someday – be just one example of many. The need to better protect digital space in the face of increased global reliance on the Internet is imperative. Moreover, these challenges can only be sustainably addressed through cooperation and coordination at all levels, including public-private sector partnerships and multistakeholder consultations. Although the crisis brought about by the pandemic is primarily connected with health institutions, the economy of a country and its critical infrastructures are also affected by the huge increase in cyberattacks. These attacks result in high costs to a nation and ultimately to the world. The developing, updating, and launching of an NCS helps combine forces of different sectors, strengthening their capacities against the potential impact of cyberattacks. An NCS offers a clear framework for all stakeholders that play a key role in the subject and a tactical scheme by defining a clear scope and timeline to establish a clear direction and improve cybersecurity in the country.

In the pursuit of sustainable solutions, it is essential to get to know the existing gaps in the cybersecurity landscape. This whole picture of the scene makes it possible to address more strategic policies and guidelines. Developing an NCS, specifically, allows a country to better coordinate and mitigate against the impact of attacks and sustainably gain a more free, open, and secure cyberspace for the medium to long term. NCSs are needed now more than ever to strategically address threats and work towards sustainable development and growth.

Example: The motivation behind NCSs in Colombia, Uruguay, and Mexico

Different reasons might kickstart a country's decision to prioritize cybersecurity and develop an NCS. These reasons include digital loans, a specific project, an incident, a political mandate, or the adoption of new technologies. For example, in Colombia, the development of the NCS stemmed from different public policy documents that the Government had issued from 2011.

In Uruguay, the NCS was created within the mandate of AGESIC (Agency for Electronic Government and Information and Knowledge Society) whose main objective is to promote the country's digital transformation and to define the Uruguay Digital Agenda.

In Mexico, the process was kickstarted by a project led by the Federal Public Administration to address the challenges of Information Technology and Telecommunications and Information Security through the generation of a manual to favor the development of ICT and security of the information. In response to this project, and as a further step in updating the guidelines to face the growing challenges in digital and cybersecurity matters, Mexico accepted the OAS' offer to receive technical support to improve national cybersecurity capabilities.

GLOBAL VS. NATIONAL GOALS

As mentioned before, the United Nations SDGs are the blueprint for achieving a better and more sustainable future for all. They address the global challenges we face, including poverty, inequality, climate change, environmental degradation, peace, and justice. All United Nations Member States adopted the SDGs in 2015 as a universal call to action to end poverty, protect the planet and ensure that all people enjoy peace and prosperity by 2030. The 17 SDGs are integrated—that is, they recognize that action in one area will affect outcomes in others and that development must balance social, economic, and environmental sustainability.

As such, during the 12th annual meeting of the Internet Governance Forum (IGF) in 2017, the community approved a new Best Practice Forum on Cybersecurity.[10] This forum explored how cybersecurity influences the ability of ICTs and Internet Technologies to support the achievement of the SDGs. They examined the roles and responsibilities of the different stakeholder groups and sought to identify policy mitigations that can help ensure the next billion(s) users can be connected safely and reliably to fully benefit from existing and future technologies. The output from this paper helps to frame the understanding that *"cybersecurity helps to build the confidence needed to motivate the use of ICTs and the Internet, and the SDGs drive that energy towards achieving the goals to end poverty, protect the planet and ensure prosperity for all."*[11]

The absence of cybersecurity capacity because of a lack of resources is a debilitating reality for developing states not limited to LAC. In 2019, Johanna Vazzana of the MITRE Corporation highlighted a report sanctioned by the Africa Cybersecurity Conference and estimated that the continent lost about $3.7 billion to cybercrime in 2017.[12] It also found that more than 90% of African businesses were operating below the cybersecurity "poverty line." This lack of cybersecurity capacity meant that they could not adequately protect themselves against losses. Official agencies were digitizing services without understanding how it could open them up to risks. The article further states that communities who need assistance reaching SDGs, through technology or otherwise, are the most fragile; they lack the resilience and safeguards that other, more resourced populations have if their security or privacy is breached. One of the conclusions Vazzana offers is that the *"sustainability of development projects and global security depend on setting new priorities and addressing some of the developing world's unique cyber risks. Another is the need to plan for cybersecurity right from the start."*[13]

THE CRITICAL ROLE OF A NATIONAL CYBERSECURITY STRATEGY

Strong cybersecurity can help support the exercise of human rights, foster economic growth, and help achieve sustainable development goals. However, the increased reliance on digital technologies and the digital and physical convergence has brought about new cyber threats to states, businesses, and individuals – online and offline. As a result, there's been a rise in measures to address these threats, manifested in a growing number of cybersecurity-related frameworks, both non-binding and binding, at the national, regional, and global levels. This proliferation of frameworks to address cybersecurity-related issues has been coupled with a proliferation of different instruments such as assessment tools, development guides, and good practices documents, among other resources.

Given the broad range of cyber threats, it becomes challenging for a country to determine which resources to use, based on effectiveness and efficiency, in order to define its cyber preparedness strategy. Some countries may focus on technical solutions, while others emphasize operations and thus the frameworks that address such threats vary in focus, scope, and structure. From our perspective, this dilemma is not without remedy given the resources and tools available, if harnessed strategically.

It's important to note that given the complexity and interrelatedness of cyber policy issues, this problem cannot be solved piecemeal but should include different types of measures. This has been recognized, for example, by the Freedom Online Coalition, whose definition of cybersecurity is framed as *"the preservation – through policy, technology, and education – of the availability*, confidentiality* and integrity* of information and its underlying infrastructure so as to enhance the security of persons both online and offline"*.[14] The mention of policy, technology, and education as core elements to foster cybersecurity illustrates the need to conceptualize cybersecurity in a holistic manner and how no single type of intervention will be able to address all types of cyber threats.

This is where an NCS comes into play. The actions taken by states and other actors to enhance cybersecurity and address cyber threats have deep links with human rights. Some measures taken to enhance cybersecurity have the clear potential to strengthen the protection of individuals' human rights, and to mitigate the risk of breaches resulting from cyber attacks, particularly when it comes to the rights to privacy and freedom of expression. In particular, an NCS can provide a structured framework to ensure a comprehensive, coordinated, and effective response to cyber threats and also to provide safeguards in the event of abuse of digital tools to infringe on these rights and general public safety. With competing priorities and limited resources, taking a strategic approach to promoting and supporting cybersecurity is the most effective and efficient way to leverage such limited resources. An NCS that is developed in collaboration with national and international stakeholders that responds to specific threats that a country is facing and clearly outlines a country's cybersecurity priorities can provide a guiding star.

With new challenges appearing every day, the need to better protect the digital space in the face of increased global reliance on the Internet has become even more imperative. An NCS can help contribute to a free, open, and secure cyberspace by providing a basis for coordination and a clear structure for stakeholders in a country to come together and address cybersecurity issues in a more strategic way.

Notes

1 Such as the SWIFT banking hack (see "2015-2016 SWIFT Banking Hack," Wikipedia, last modified February 27, 2022, https://en.wikipedia.org/wiki/2015%E2%80%932016_SWIFT_banking_hack., the COVID-19 pandemic (see OECD, Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides, Digital Economy Outlook 2020 Supplement, (Paris, OECD, 2020), https://www.oecd.org/digital/digital-economy-outlook-covid.pdf., and the colonial pipeline ransomware attack (see William Turton and Kartikay Mehrota, "Hackers Breached Colonial Pipeline Using Compromised Password," Bloomberg, June 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

2 S. Creese, W. H. Dutton, P. Esteve-González, and R. Shillair "Cybersecurity capacity-building: cross-national benefits and international divides," Journal of Cyber Policy 6:2, 214-235, DOI.

3 Frank La Rue, UN. Secretary-General, UN. Human Rights Council. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, "Promotion and protection of the right to freedom of opinion and expression : note / by the Secretary-General," A/66/290, Report of the Special Procedure of the Human Rights Council, United Nations, August 10, 2011, https://digitallibrary.un.org/record/710170?ln=en.

4 "The 17 Goals," United Nations, Department of Economic and Social Affairs, Sustainable Development, accessed 21 April 2022, https://sdgs.un.org/goals.

5 United Nations, "Report of the Secretary-General, Roadmap for Digital Cooperation", United Nations, June, 2020: 5, https://www.un.org/en/content/digital-cooperationroadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf.

6 Ibid.

7 "Transforming our world: the 2030 Agenda for Sustainable Development," United Nations, Department of Economic and Social Affairs, Sustainable Development, accessed August 30, 2021, https://sdgs.un.org/2030agenda.

8 Robert Morgus, "Securing Digital Dividends: Mainstreaming Cybersecurity in International Development," New America, last modified April 23, 2018, https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/.

9 Cedric Nabe, "Impact of COVID-19 on Cybersecurity," Deloitte, accessed August 30, 2021, https://www.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

10 "Proposal for 2017 Best Practice Forum (BPF) on Cybersecurity," Internet Governance Forum, accessed August 30, 2021, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/625.

11 "IGF 2017 - Best Practice Forum on Cybersecurity," Internet Governance Forum, accessed August 30, 2021, https://www.intgovforum.org/multilingual/content/igf-2017-best-practice-forum-on-cybersecurity.

12 Johanna Vazzana, "Securing Technology is No Longer a 'First World Problem' Why it's critical to address the growing cybersecurity risks in the developing world," New America, February 19, 2019, https://www.newamerica.org/cybersecurity-initiative/humans-of-cybersecurity/blog/securing-technology-is-no-longer-a-first-world-problem/.

13 Ibid.

14 "Why Do We Need a New Definition for Cybersecurity?," The Freedom Online Coalition, accessed September 10, 2021, https://freedomonlinecoalition.com/blog/why-do-we-need-a-new-definition-for-cybersecurity/.

Part **2**

PAVING THE WAY FOR YOUR COUNTRY

Part Two of this document focuses on stakeholder engagement and leadership in NCS development. The authors explore the value of stakeholder engagement and provide guidance to identify relevant stakeholders to include in an NCS process, providing examples of stakeholder engagement in NCS development processes in the Americas. The authors also address the need for leadership in the process and different possible government structures based on examples from the region.

THE IMPORTANCE OF A MULTISTAKEHOLDER APPROACH

As stated in Part One, strong cybersecurity can help individuals exercise their rights, as well as address the increasing prevalence, sophistication, and severity of cyber threats. This potential influence on human rights and the ability to respond to cyber threats makes having a comprehensive NCS in place critical to a nation's economic and social well-being. Addressing all the different cybersecurity challenges that a country faces, however, makes developing NCSs and other related policies particularly challenging. That is why an inclusive approach to cybersecurity can add value by leveraging a broad and rich set of expertise and engaging a broader set of stakeholders in the process of developing and implementing NCSs.

Inclusive or multistakeholder approaches to policymaking are not new. They have been tested and applied in other policy spaces like extractive industries, environmental policy, conflict prevention, and peacebuilding, among others.[15] In the field of cybersecurity policy, the need for effective cross-stakeholder collaboration is widely recognized, with numerous international instruments reinforcing the message. For example, the London Process, which started in 2011 in the UK and resulted in a series of Global Conference on CyberSpace meetings, has consistently highlighted the need for multistakeholder engagement and cooperative approaches to cybersecurity challenges.[16] It has also been highlighted in outcome reports from UN processes such as the UN Group of Governmental Experts and the Open-Ended Working Group.[17]

In the recently published guide from ENISA, the study found that it is difficult for governments to understand the needs of the industry, as well as to develop expertise in dealing with Public-Private Partnerships.[18] Further, the study highlighted that dedicated funding mechanisms and initiatives often focus on varied research and innovative objectives rather than being specific on cybersecurity. This suggests there is a need to remind policymakers to consider different cybersecurity needs across sectors and develop sector-specific innovation priorities at the national and regional levels.

Cybersecurity is not a dedicated area of a selected group of experts or a specific sector, but rather is a cross-cutting issue that affects or involves all actors using ICTs and engaging in cyberspace (see the Maritime Sector for a case study later in this). Equally, cybersecurity as a topic is very broad and comprises several sub-topics, like policy, strategy, and legal frameworks, critical infrastructure protection, cybersecurity awareness, cybercrime, and standards. For an NCS to be developed, the expertise of different stakeholders will be needed throughout the development and implementation process.

While there is intrinsic value when it comes to involving a wide range of stakeholders in cybersecurity processes, two of the more practical reasons why engaging stakeholders into the NCS process specifically can add value are:[19]

1 Stakeholder engagement can lead to a more informed NCS.

As a question of public policy, cybersecurity affects a range of different topics. It is unlikely that a single actor could hold all the expertise needed to address cyber issues, and so several stakeholder groups with different experiences are needed to bring their unique expertise and value to the discussion. For example, the private sector will have a unique understanding of the cyber threats businesses face, products and services being developed to address them, and the market impact of policy proposals. The technical sector will be uniquely positioned to address concerns around critical infrastructure protection and standards. Civil society organizations can analyze the human rights implications of different policies under consideration as well as the different cybersecurity threats faced by different groups within society and offer insight on capacity-building efforts.

2 Stakeholder engagement leads to buy-in, which may result in a more effective implementation of the NCS.

A diverse set of stakeholders will be involved in the implementation of any NCS and other cyber policies. For example, almost all NCSs contain sections on public-private partnerships, research and development funding, and public awareness-raising, all of which involve non-governmental stakeholders. Successful and effective implementation of cyber policies relies, in part, on building trust and coordination among the parts. Stakeholders who have been involved in developing an NCS will have a stronger understanding of the strategy and what is required from them. This understanding can, in turn, make implementation efforts more effective. Equally, without providing an opportunity for input, implementation of policies such as these may be perceived by stakeholders as an imposition. When it comes to reviewing an NCS, the feedback and information provided by various stakeholders is vital; this input is much more likely to be forthcoming if those stakeholders have been part of the NCS's development and implementation.

Multistakeholderism in practice: the examples of Colombia, Mexico, and Belize

In Colombia, the OAS supported the process closely and provided expert advice for developing the NCS. The team defined a roadmap document for the formulation of the policy, incorporating contributions from different stakeholders regarding their priorities and expected participation in the development of the NCS.

There were two consultation periods - the first ran from 11 October to 8 November 2019, and approximately 260 comments were received from 30 entities. The second consultation period was open from February 25 to March 10 and gathered around 351 comments from 24 entities. Additionally, roundtables were held with key actors of the digital ecosystem, receiving comments and feedback. The participation of private companies, non-governmental organizations (NGOs), telecommunications network and service providers, and academia, both national and international, was facilitated.

In the initial stages of the development of Mexico's NCS, a Technical Assistance Mission, coordinated by the Organization of American States (OAS) in April 2017, gathered diverse experts and stakeholders in roundtable discussions to better understanding Mexico's cybersecurity requirements and evaluate best practices in order to help develop a national framework for the cybersecurity strategy. This gave the process access to expert opinion and greater resources, including a set of recommendations to guide the drafting of the NCS.[20]

In Belize, the government established a multistakeholder NCS Task Force under the leadership of the government's National Security Council Secretariat (NSCS) and with the support of the Organization of American States Inter-American Committee against Terrorism (OAS/CICTE) Cyber Program. The Task Force comprised 15 different entities, ranging from governmental stakeholders and the private sector to civil society and academia.

Once a first draft was developed by the dedicated multistakeholder Task Force, the government undertook an open online consultation to gather stakeholder feedback on the text. The text of the first draft was published online on the Belize Crime Observatory Website. The draft was open for comments, suggestions, and edits from stakeholders for three weeks. In addition to this, the government shared the strategy draft via email, inviting specific stakeholders to submit input and be part of in-person public consultative and validation workshops. Having the opportunity to provide input online made the process more accessible to those stakeholders unable to participate in in-person consultations.

IDENTIFYING STAKEHOLDERS

Different stakeholders may be involved in different ways and at different stages of the NCS development, implementation, and/or review; it is important to map and identify *relevant* stakeholders early in the process.

All stakeholders are relevant when it comes to cybersecurity because everyone has an interest and need for ensuring a free, open, and secure cyberspace. But when it comes to cybersecurity policymaking more specifically, relevant stakeholders tend to refer to:

- Those with a mandate, role, or responsibility in the process;
- Those with skills or expertise needed to inform the policy and operationalize with; and
- those who could be disproportionately affected by the policy or its implementation.[21]

These stakeholders may belong to a range of stakeholder groups, including:

- Different government departments, particularly those dealing with national security and resilience, defense, foreign affairs, and relevant infrastructures such as ICT and energy;
- Other public bodies whose mandate also includes the above issues, such as telecommunications regulators;
- The judiciary and law enforcement;
- Academic institutions whose expertise includes cybersecurity, such as universities, research entities, think tanks, and independent experts and researchers;
- Civil society organizations, particularly those with expertise in human rights, those who engage with different groups and communities within society vulnerable to cyberattacks, those which engage directly with the public on cybersecurity-related issues, and networks and umbrella groups;
- International and regional organizations whose mandate or expertise includes cybersecurity, such as the ITU, the Organization of American States, or The World Bank;
- The technical community, including members of the incident response community, standard-setting organizations, and domain name systems; and
- The private sector, including trade associations, particularly those from industries and sectors that are especially vulnerable to cyber threats, or develop technology or provide services that enhance cybersecurity.

Figure 1 **Different stakeholder groups to engage in NCS development**[22]

GOVERNMENT	ACADEMIA	CIVIL SOCIETY	INTERGOVERNAMENTAL/ INTERNATIONAL ORGANISATIONS	TECHNICAL COMMUNITY	PRIVATE SECTOR
Relevant ministries (ICT), Economies, etc.)	Universities;	Interest-driven groups (e.g. human rights or child online protection);	Regional organisations (e.g. African Union, OAS, Council of Europe);	CSIRTs/CERTS;	Technology and networking companies;
Regulatory agencies;	Research entities and think tanks;	Identity-based groups (e.g. faith, minority, or women's rights);	International organisations (e.g World Bank, ITU).	Standarisation organisations;	Information security companies;
Judiciary and law enforcement;	Independent researchers and experts.	CSO networks and umbrella groups.		Domain name system.	Business associations.
Defense and security services.					

Case study: Civil Society Engagement in the Development of Chile's National Cybersecurity Policy

By Derechos Digitales

In 2014, Michelle Bachelet, then president of Chile, proposed creating a national cybersecurity policy, a term often used interchangeably with "national cybersecurity strategy." A participatory process was designed, which contemplated the participation of different stakeholders and was led by a group created especially for this purpose in April 2015: the Inter-ministerial Committee on Cybersecurity (CICS). Stakeholders would be active participants, and their views effectively helped shape the policy.

The first stage of this collaborative process was the submission of the document entitled *Bases for a National Cybersecurity Policy*, published in March 2015 jointly by the Ministries of the Interior and Defense. The document was published to establish the need for a national policy, define its theoretical framework, and lay out the full process agenda. The CICS invited select stakeholders to different meetings to provide feedback on topics covered in the document, propose additions, and solve questions.

After these meetings, the CICS started drafting the National Cybersecurity Policy (NCSP), taking into consideration the feedback received. A first draft of the NCSP was published in February 2016 and submitted for public consultation between 29 February and 18 March 2016, when written comments to the policy draft were received. This stage saw contributions from 43 entities, a considerable number in comparison to other processes of cyber policy. From the respondents, four were representatives of academia, three from the technical community, seventeen from the private sector, eight from public agencies, seven from civil society organizations, and four unaffiliated individuals.

As expected, the comments from each stakeholder focused mainly on their area of interest. However, as a result, different visions and concerns were incorporated into the document. This diversity of perspectives contributed to a broad acceptance of the document, as well as its endurance. Even though it was an opposition government, the government that succeeded Michelle Bachelet's continued with the implementation of this NCSP as if it were its own, without trying to modify it, thus demonstrating a successful case of public policymaking.

It is important to note that although this was not the first policy draft open to different forms of stakeholder participation, it was one where participation was perceived as useful and effective by the same stakeholders. The leading role by the CICS was fundamental, by directly seeking participation from different stakeholders and engaging in efforts to facilitate participation of stakeholders located outside the capital. This effort was perceived and recognized by the participants, who were able to see their contributions reflected in the final version of the NCSP. A comparison between the Bases document, the draft policy, and the final PNCS shows that changes were indeed made based on the feedback provided in the consultation.

The process of elaboration of the Chilean NCSP demonstrates the importance of considering the voices of different actors in the elaboration of public policies. The wider acceptance of its outcomes and the recognition of the process itself are valuable examples of open and participatory policymaking. Whether the policy is brought to completion within its projected timeframe (2017 to 2022) remains to be seen, but the template for a new process is already set.

Case study: Civil society's contribution to Colombia's vulnerability disclosure protocols

By Karisma Foundation

Despite challenges, Colombia has been evolving its national cybersecurity policy from a focus on national security and defense to the construction of trust among multiple stakeholders and the recognition of the economic and social function of digital security to enhance the well-being of individuals and of societies as a whole.

One element that Karisma Foundation has been engaging in over the past few years has been cybersecurity threats and vulnerability disclosure.

In 2011 the national cybersecurity policy in Colombia created the Group for Response to Cyber Emergencies of Colombia (colCERT), which responded to the Ministry of National Defense. In 2016, Karisma started a digital security research and advocacy project to develop a civil oriented and multistakeholder approach to vulnerability response, analyzing government transactional websites to evaluate the information they provide to citizens, their level of digital security, and how they protect privacy and identify vulnerabilities. The purpose of these analyses was to contribute to the improvement of websites to benefit both the citizens and the entities responsible for these sites, and find a trusted path with the government to inform them and for vulnerabilities to be effectively addressed. A key purpose has also been to advocate for a coordination path that would be open to all stakeholders.

For this purpose, Karisma conducted audits of several government websites and also mobile apps, and found vulnerabilities in them. In 2017 Karisma submitted the second report to the Ministry of ICT and the Unit for Integral Attention and Reparation to Victims (UARIV), which sparked a positive reaction by the Government and allowed a collective effort to emerge, leading to the implementation of a plan to improve the site's digital security. The exercise was published during the National Digital Security Forum organized by the Government in 2017 as an example of collaboration and shared responsibility between civil society and the Government, which was identified as a good practice under international standards.[23]

After several other exercises in 2019 Karisma also produced a report analyzing how coordinated disclosure of vulnerabilities were implemented in the world and what were the barriers in Colombia for a formal implementation of such protocol.[24]

The development of Colombia's new digital security strategy, which was finalized in 2020, provided the momentum for the government to review Karisma's work on the state of the art in the matter in Colombia and to articulate it with the work that was being developed at Organization for Economic Co-operation and Development (OECD). This all led to the inclusion of specific actions to enable responsible disclosure in the country and ensure response and due diligence in responding to vulnerabilities. Currently, ColCERT is the lead authority for Colombia's national response to digital security threats including vulnerability treatment that replicates the original vision, and the Ministry of Defense is responsible for the development of a response through an institutional coordinator, however there is now an open channel of communication that can help them address these issues through increased collaboration with other stakeholders, including the Ministry of Information Technologies or the Delegation of Data Protection.

The next step and priority will be its implementation. In the meantime, the process was recognized by the OECD on its work on vulnerability response in 2021 as a good practice and as such is expected to serve as a driver for the Colombian government to make further progress on it.[25]

The value of research and the role of academia in NCS development.

As specified earlier in this section, academic institutions such as universities, research entities, think tanks, and independent experts and researchers are relevant stakeholders who can have an important role in the NCS development process. The research that academia can undertake can be a powerful tool to leverage and contribute evidence-based arguments and provide a neutral academic position to inform cyber policymaking processes and capacity-building efforts.

The need for further research on cyber policy issues is evidenced by an increase in research efforts, such as the newly established Research Agenda at the Global Forum on Cyber Expertise.[26] The value of research has also been recognized by countries around the world, like the UK, who in 2020 published a study looking at its position as a world leader in cybersecurity research.[27] The study highlighted how a long-term focus on research could help foster leadership in cybersecurity and concluded that although significant capacity had been developed in the UK in the last decade, there was a need for a step-change in investment in cybersecurity research in various forms (such as strategic clusters of excellence, doctoral training and the creation of national research facilities) in order to create sustainability and maintain the UK's cybersecurity research position in the world. The UK further recognizes research and academia as one of the elements under the pillar of Education & Skills in the UK National Cybersecurity Centre.[28]

DIFFERENT MODELS OF LEADERSHIP

When starting the process of developing its NCS, a country must establish who will lead the process. The leading body might be an existing agency, a new team with a specific mandate to lead on the process, or even a multi-agency group. In many cases, the leading agency will belong to the government's executive power, given that cybersecurity at the national level is normally in the interest of public security. In addition to providing leadership to move the process forward, it is also crucial that the leadership ensure collaboration within government and across stakeholder groups to promote a smooth implementation. Therefore, the lead for this process is usually vested with sufficient authority and competence and often plays the role of interlocutor and coordinator.

There are different approaches to promote leadership in the process and ensure coordination. Below are examples from Colombia, Mexico, Uruguay, and Belize.

Colombia

In the case of Colombia, the process was led mainly by the Administrative Department of the Presidency of the Republic, the Ministry of Information Technologies and Communications, the Department National Planning, and the Ministry of National Defense, with support from other governmental bodies like the Office of the Attorney General of the Nation, the National Intelligence Directorate, and the Ministry of Foreign Relations. The drafting was led by the National Planning Department and the Ministry of Information Technologies and Communications, in coordination with the Presidential Council for Economic Affairs and Digital Transformation, which is the body that generates high-level commitment in the entities. Additionally, they worked with multidisciplinary roundtables that brought together actors from civil society, academia, the private sector, unions, and public entities, who contributed to drafting the document.

Its approval is given through the National Council for Economic and Social Policy, which is the highest national planning authority and acts as an advisory body to the government in all aspects related to the economic and social development of the country.

Mexico

In Mexico, the leadership of the process was in the hands of the Executive Power (within the office of the Presidency), with the initial support of the National Security Forces, taking into account the objectives established in the National Development Plan mandated by the Political Constitution.

To ensure coordination, Mexico appointed a leader for each strategic objective and a leader for each transversal axis. Each leader brought together different actors or stakeholders (academia, civil society, companies, NGOs, etc.) according to the theme to detect needs and establish collaboration agreements. Later the leaders of the transversal axis had cross-sectional meetings with each of the leaders of the strategic objectives to establish specific objectives and lines of action in each strategic objective corresponding to each transversal axis in order to achieve orderly collaboration of the different stakeholders of Mexican society in each strategic objective.

Recently Mexico published a revised National Digital Strategy 2021-2024, focused on improving and bring harmony to its regulatory framework, the maximization of infrastructure use, and an approach based on information security, the integration of information for management efficiency, as well as improving access to areas without coverage.[29]

Uruguay

In Uruguay, the process was led by the governmental Agency for Electronic Government and Information and Knowledge Society (AGESIC), which was regulated by a decree. AGESIC belongs to the Presidency of Uruguay; this positioning was key to the support that was achieved in the strategy and, with it, in the agency's projects.

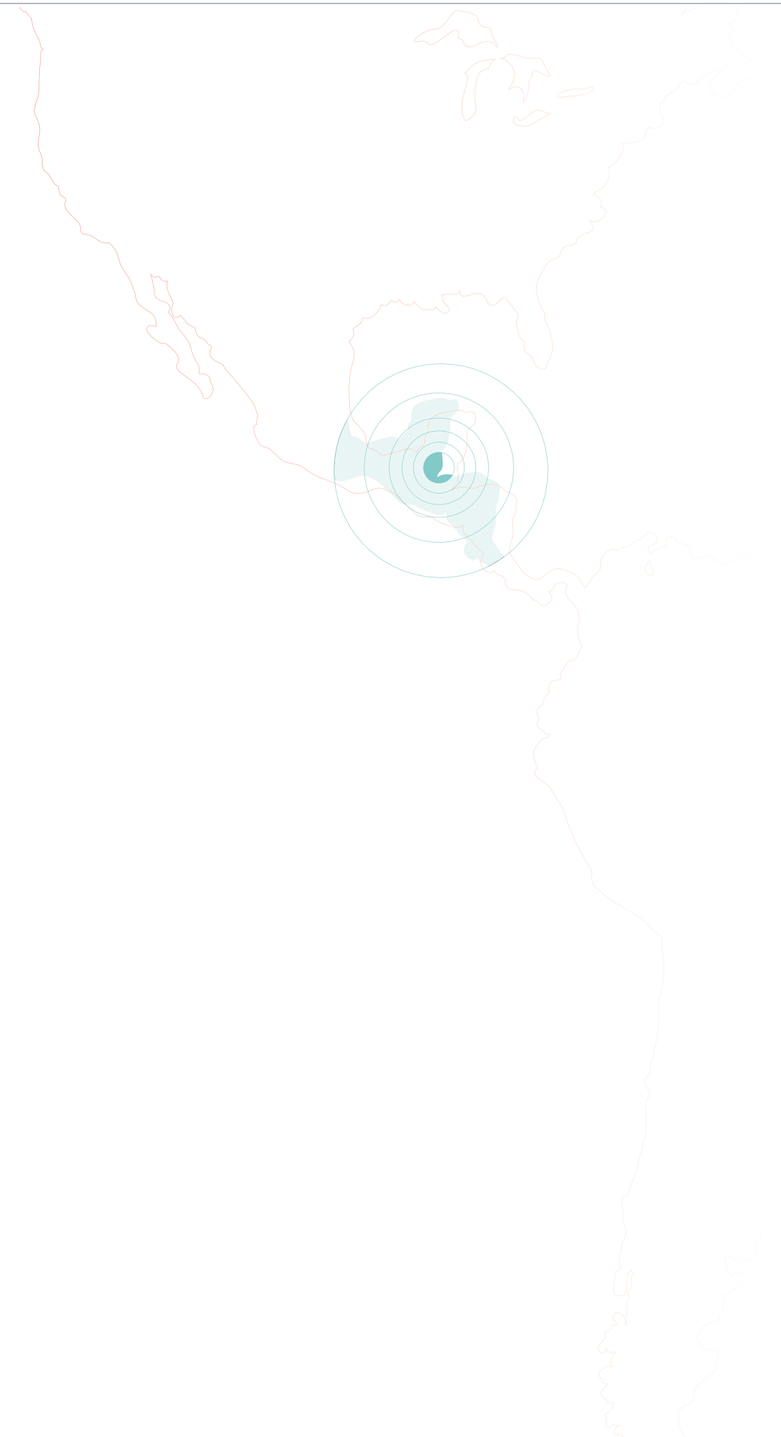
Subsequently, the Accountability Act of October 2006 complements the list of objectives, adding that of conceiving and developing a national policy on Information Security issues that allow the prevention, detection, and response to incidents that may affect the country's critical assets. Similarly, this regulation creates the function of "Executive Director of the Agency for the Development of the Government of Electronic Management and the Information Society", considered a high priority and whose responsibility will be the operational structure of the agency.

Today AGESIC has 4 divisions in the Information Security Directorate:

- Cybersecurity Incident Response Center (CERT)
- Cybersecurity Operations Center (SOC)
- Information Security Management and Audit.
- Electronic Identification

In Uruguay, the Council for the Information Society coordinated by AGESIC meets periodically throughout the year to monitor the Uruguay Digital Agenda (Agenda Uruguay Digital or AUD). The agency's Information Society area prepares a monitoring report for each meeting, obtaining data from each person in charge (AGESIC among them). In AUD's goals some initiatives are components of projects that have dependencies of various organizations. During the monitoring meetings, different alternatives are agreed to organize transversal activities, such as making known those responsible for each organization's project, promoting communication between them or, in some cases, even forming project teams made up of specialists from different organizations. At the AGESIC strategic plan level, some projects are transversal to the government. The agency promotes the creation of mixed teams made up of heads of each of the agencies involved.

Additionally, AGESIC has roles dedicated to each of the State agencies in order to promote alignment at the transversal level and achieve better results in each project. AGESIC's Information Security area promotes the development and strengthening of an ecosystem together with the public, private, and academic sectors that aim to promote the subject's development, sharing initiatives, knowledge, research, training, and development. In this way, multiple initiatives and activities are generated with different sectors, seeking greater synergy in the ecosystem.



Belize

In Belize, the government established a multistakeholder NCS Task Force under the leadership of the government's National Security Council Secretariat (NSCS) and with the support of the Organization of American States Inter-American Committee against Terrorism (OAS/CICTE) Cyber Program. The Task Force comprised 15 different entities, ranging from governmental stakeholders and the private sector to civil society and academia.

It was formed in mid-2017, after the first National Cybersecurity Symposium, and started coordination to develop the strategy in 2018. The Task Force held around ten different meetings throughout the process.

In addition to leading on the drafting of the strategy, the Task Force played a key role in helping shape capacity-building efforts, which were aimed at building the capacity of non-governmental stakeholders to engage in the development of the strategy. The Task Force is still active and is expected to remain engaged in the NCS implementation.

Notes

15 See for example the Internet Assigned Numbers Authority (IANA) transition in 2016, which enabled the United States Government to transfer its clerical and stewardship roles in the Domain Name System to the multistakeholder community: "IANA Transition," Internet Society, accessed August 30, 2021, https://www.internetsociety.org/iana-transition/.

16 "London Process," Wikipedia, last modified July 16, 2021, https://en.wikipedia.org/w/index.php?title=London_Process&oldid=1033933206.

17 See for example, "Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015," submitted by the United Kingdom's Multi-stakeholder Advisory Group on Cyber issues, accessed on April 21, 2022, https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf. and Digital and Cyberspace Policy Program and Net Politics, "A Multistakeholder Meeting at the United Nations Could Help States Develop Cyber Norms," Council on Foreign Relations, January 16, 2020, https://www.cfr.org/blog/multistakeholder-meeting-united-nations-could-help-states-develop-cyber-norms.

18 ENISA, "Good practices in innovation on Cybersecurity under the NCSS," ENISA, 2019, https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.

19 Additional reasons are described in the Global Partners Digital, "Toolkit for Inclusive and Values-Based Cybersecurity Policymaking" Global Partners Digital, March, 2020, https://www.gp-digital.org/publication/toolkit-for-inclusive-and-value-based-cybersecurity-policymaking/.

20 OAS Technical Assistance Mission, "Recommendations for the Development of the National Cybersecurity Strategy," OAS, April, 2017, http://www.oas.org/documents/eng/press/Recommendations-for-the-Development-of-the-National-Cybersecurity-Strategy.pdf.

21 Additional information is available in Global Partners Digital, "Multistakeholder Approaches to National Cybersecurity Strategy Development," Global Partners Digital, June, 2018, https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf.

22 Ibid.

23 "La Corresponsabilidad en Acción", Fundación Karisma, August 31, 2017, https://web.karisma.org.co/la-corresponsabilidad-en-accion/.

24 Stéphane Labarthe, Estudio Sobre Rutas de Divulgación en Seguridad Digital, (Bogota, Fundación Karisma, 2019) https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf.

25 https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf.

26 Global Forum on Cyber Expertise (GFCE), "Global Cyber Capacity Building Research Agenda 2021," GFCE, November 25, 2020, https://thegfce.org/the-global-cyber-capacity-building-research-agenda-2021-is-now-online/.

27 Max Swinscow-Hall, "The future of the UK's Cyber Security Research Position in the World," Imperial College London, September 7, 2020, https://www.imperial.ac.uk/news/202413/the-future-uks-cyber-security-research/.

28 "Education & Skill," National Cyber Security Centre, accessed August 30, 2021, https://www.ncsc.gov.uk/section/education-skills/research-and-academia.

29 Secretaría de Gobernación, "Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024", Diario Oficial de la Federación, June 9, 2021, https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021.

Part **3**

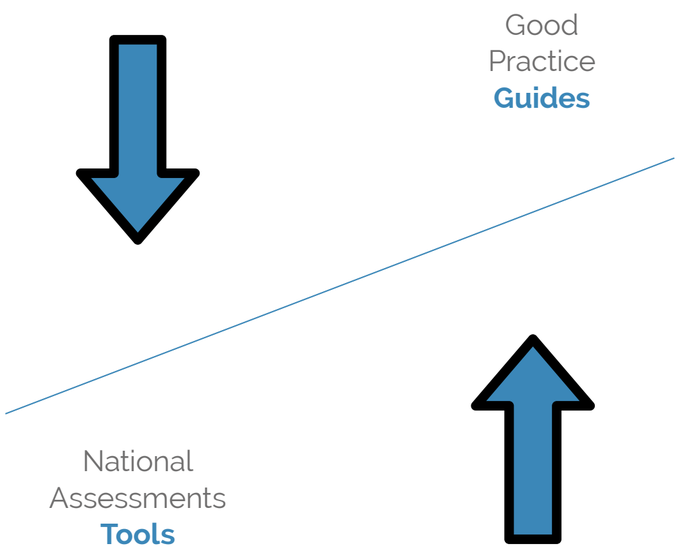
NATIONAL CYBERSECURITY STRATEGY RESOURCES

There are a variety of approaches to developing an NCS. Strategies themselves can differ in their intent and complexity, from high-level frameworks through which future cybersecurity policies and processes will be addressed to detailed cybersecurity strategies that prescribe the structures, policies, and mechanisms for achieving cyber-readiness and maturity. This section reviews some of the available assessment tools and best practice guides, providing useful and valuable information about each one and resources for analyzing, defining, and deciding which to utilize. The tools and guides are not mutually exclusive; stakeholders may find a mix or combination of several will best serve their country's specific requirements.

According to *Motivating Organizational Cyber Strategies in Terms of Preparedness* by Deborah Bodeau and Richard Graubart, these frameworks and guidance vary based on the nature of the cyber threat.[30] For instance, some explicitly assume traditional threats. Others, while mentioning advanced threats, do not consider the resistance against ongoing, stealthy campaigns to be necessary. Some focus on technical solutions, while others emphasize operations. This diversity makes it very challenging for an organization to determine which resources to use, based on effectiveness and efficiency, in order to define its cyber preparedness strategy. This dilemma is not without remedy given the resources and tools available, if harnessed in a strategic manner. The tools should be used as an aid to develop an NCS, not as absolute checklists to follow.

One of the key distinctions in the initial stages of the development process is to distinguish an assessment tool from a guide.

Figure 2 **Guide vs. Assessment Tools**



An assessment tool is usually built around a maturity model framework that provides a methodology for evaluating and assigning a maturity level to a grouping of security processes based on specific criteria; this answers the question of why an NCS is needed. Comparatively, a guide gives you a systemic way to answer the question of how to develop an NCS. Overall, it is important to distinguish the 'why' vs. the 'how' in order to be strategic in your decision-making at every stage.

ASSESSMENT TOOLS

There are several tools available to assess cyber capacity in a country[31]. The tools are not mutually exclusive; it will depend on the purpose for which it needs to be used. Regardless of the tools or guides chosen, it is important to map and assess threats, vulnerabilities and gaps, risks, capacities, supply chain, stakeholders, and so on.

Some of the most known tools include:

- *Combating Cybercrime Capacity Building Assessment Tool*, by The World Bank;[32]
- Cyber Readiness Index 2.0, by The Potomac Institute for Policy Studies;[33]
- *Cybersecurity Capacity Maturity Model for Nations*, by the Global Cyber Security Capacity Centre;[34]
- *Global Cybersecurity Index*, by the International Telecommunication Union;[35]
- *National Cybersecurity Index*, by the e-Governance Academy;[36]
- *National Cybersecurity Strategies Evaluation Tool*, by ENISA;[37] and
- *National Cybersecurity Framework Manual.*[38]

Combating Cybercrime Capacity Building Assessment Tool – The World Bank

Through its assessment tool, The World Bank enables countries to evaluate their current capacity to combat cybercrime and identify capacity-building priorities.[39] Its main purpose is to allow a user to determine gaps in capacity and highlight priority areas to direct capacity-building resources. This global tool is oriented to policymakers, legislators, law enforcement authorities, civil society in developing countries, and any other interested individual, and it is focused on nine (9) dimensions. These dimensions are:

1. Non-Legal Framework (national strategies and policies and other matters of a non-legal nature such as cooperation with the private sector);
2. Legal Framework (national law and whether a country has joined a treaty; Substantive Law, addressing activities that have been criminalized);
3. Procedural Law (investigatory matters);
4. e-Evidence (admissibility and treatment of digital evidence in the cybercrime context);
5. Jurisdiction (how the jurisdiction of the crime is determined);
6. Safeguards ("due process", data protection, and freedom of expression);
7. International Cooperation (extradition and both formal and informal levels of MLA); and
8. Capacity building (institutional (e.g., law enforcement training academies) and human capacity-building, training needs for law enforcement, prosecution, and the judiciary).

This assessment tool enables effective and universally applicable evaluation of a nation's cybercrime preparedness by ensuring *objectivity, richness*, and *ease of comprehension*. The combination of these three elements facilitates policy, law, and decision-makers to best decide how resources should be allocated. *Objectivity* is achieved by making the response to each question in the assessment tool a binary (yes/no) response to the greatest extent possible or to create a clear choice along a small-scale of options. *Richness* is achieved by weighting each criterion. It uses approximately 115 indicators grouped into nine themes (or dimensions). *Ease of comprehension* is achieved through graphic representations of assessment in a single "spider" chart. The chart helps each country to identify whether its current practice corresponds with international good practices. Each dimension on the general spider chart can also be drilled down to a more granular level, showing performance on each of the different sub-criteria. This tool's use and results are for the benefit of the person downloading it and can be self-administered. According to the site, workflow remains solely with the user; there is no tracking, ranking, or reporting back of results.

Cyber Readiness Index 2.0 (CRI 2.0) - The Potomac Institute for Policy Studies

The CRI 2.0 is a methodology to evaluate and measure a country's preparedness levels for certain cybersecurity risks. [40] The CRI 2.0 is designed to provide a compelling and actionable review of a country's policies, plans, laws, standards, market levers (e.g., incentives and regulations), and other initiatives. The

beneficiaries of this tool are global leaders, national and regional governments, ministries or government agencies, cybersecurity agencies and policymakers, academia, cybersecurity experts, and individual researchers. The CRI 2.0 uses over 70 unique indicators across seven (7) essential elements to discern operationally ready activities and identify areas for improvement. The seven categories are the following:

1. **National Strategy** (publication of national strategy, designation of competent authority, identification of key government entities and key commercial entities responsible for plan, mechanisms to secure critical infrastructure, identification of critical services, identification of national standards for continuity of service);
2. **Incident Response** (publication of incident response plan, identification of cross-sector dependencies, evidence plan is exercised and updated, publication of cyber threat assessment, establishment of CSIRT, financial and human resources);
3. **E-crime and Law Enforcement** (ratification of international cybercrime treaty, efforts to reduce e-crime, institutional ability to fight cybercrime, commitment to review existing laws and mechanisms, efforts to clean up infected infrastructure; law enforcement training and capability development);
4. **Information Sharing** (policy of information sharing, institutional structure to share information with government agencies and/or industry, evidence of cross-sector and cross-stakeholder coordination mechanisms, ability, and process for government to declassify intelligence information);
5. **Investment in R&D, Education, and Capacity** (government incentive mechanisms to encourage cybersecurity innovation and investments, financial and human resources for R&D and technology transfers, degree programs in cybersecurity, sponsorship of cybersecurity awareness campaign and educational programs);
6. **Diplomacy and Trade** (identification of cybersecurity as essential element of foreign policy and international economic negotiations, establishment of dedicated personnel in countries' foreign offices dedicated to cyber diplomacy, participation, and enforcement of international, multi-national, regional cybersecurity agreements); and
7. **Defense and Crisis Response** (establishment of national-level military and/or nonmilitary organization for cyber defense, evidence of national-level cyber exercises with commercial partners and/or international partners, establishment of standards for responsible state behavior in cyberspace, establishment of rapid assistance mechanisms).

According to Melissa Hathaway, author of the CRI 2.0, few countries have aligned their digital agenda with their cybersecurity plans. The CRI seeks to incentivize this alignment by bringing attention to each country's Internet-infrastructure dependencies and vulnerabilities and highlighting the national economic erosion caused by cyber insecurity.[41]

While the general description of the tool can be downloaded, this tool is not self-administered; it is applied by the team of experts from the CRI team.

Cybersecurity Capacity Maturity Model for Nations (CMM) - Global Cybersecurity Capacity Centre (GCSCC)

The CMM facilitates benchmarking a country's cybersecurity capacity across five dimensions and enables nations to self-assess, plan investments and NCSs, and set priorities for capacity development.[42] A CMM review aims to gather data about the country's cybersecurity capacity landscape and determine which of the five stages of cybersecurity maturity the country has reached across the CMM dimensions. This tool is publicly available.

The five dimensions, which are crucial to building a country's cybersecurity capacity, are:

1. **Cybersecurity Policy and Strategy** (national cybersecurity strategy, incident response, critical infrastructure (CI) protection, crisis management, cyber defense, communications redundancy);
2. **Cyber Culture and Society** (cybersecurity mindset, trust, and confidence on the Internet, user understanding of personal information protection online, reporting mechanisms, media, social media);

3. **Cybersecurity Education, Training and Skills** (awareness-raising, framework for education, framework for professional training);
4. **Legal and Regulatory Frameworks** (legal frameworks, criminal justice system, formal and informal cooperation frameworks to combat cybercrime); and
5. **Standards, Organizations, and Technologies** (adherence to standards, Internet infrastructure resilience, software quality, technical security controls, cryptographic controls, cybersecurity marketplace, responsible disclosure).

The assessments are conducted through the following process. Once a country has been identified for a CMM review, the review team establishes a working relationship with a 'local host' and starts conducting contextualizing desk-research, while the host identifies stakeholders and schedules consultations in coordination with the review team. During the following stage, the review team and the local host meet in country to conduct a three-day consultation process with the stakeholders identified. During the review sessions each stakeholder cluster engages in open discussions and answers questions that relate to one or two Dimensions of the CMM. Any gaps that emerge during the in-country data-collection process are bridged by either subsequent desk research or remote follow-up sessions with the stakeholders. Finally, once the review has been conducted, a report is produced by the researchers of the review team. This report describes the in-country cybersecurity context, summarizes the findings for each factor and aspect, outlines the stages of cybersecurity capacity maturity and provides peer-reviewed recommendations that enable the country to enhance its cybersecurity capacity. Based on the assessment results, a country can define which of the five stages of maturity the country has achieved in each previously described dimension: *start-up*, *formative*, *established*, *strategic*, and *dynamic*.

The data is used to produce an evidence-based report that is submitted to the government with recommendations to benchmark the maturity of a country's cybersecurity capacity; detail a pragmatic set of actions to contribute to the advancement of cybersecurity capacity maturity gaps; identify priorities for investment and future capacity-building; build business cases for investment and corresponding expected national cybersecurity performance enhancements. Implementers administer this tool in collaboration with the GCSCC.

Global Cybersecurity Index (GCI) -The International Telecommunication Union (ITU)

The Global Cybersecurity Index (GCI) supports countries in identifying areas for improvement in the field of cybersecurity, including identifying gaps in cybersecurity development between nations and regions and raising awareness regarding cybersecurity worldwide.[43] The assessment also helps indicate which countries need the most support to improve their cybersecurity posture. Through the data collected, the GCI highlights and promotes practices ITU Member States can implement suitable to their national environments and fosters a global culture of cybersecurity.

Its main beneficiaries are Member States' ministries and agencies, cybersecurity agencies and policymakers, academia, cybersecurity experts, and any interested individuals.

Topics covered in the GCI include:

- Legal Measures (cybercrime substantive laws, cybersecurity regulations);
- Technical measures (national/government incident response teams, sectoral CERT/CIRT/CSIRT, national framework for the implementation of cybersecurity standards, child online protection (COP));
- Organization Measures (national cybersecurity strategies (NCS), responsible/national agencies, cybersecurity metrics);
- Capacity-Building Measures (public awareness campaigns, cybersecurity training for professionals, national education programs and academic curriculums, cybersecurity research and development programs, national cybersecurity industry, government incentive mechanisms to support cybersecurity development); and
- Cooperation Measures (bilateral agreements, participation in international mechanisms (forums), multilateral agreements, public-private partnerships, inter-agency partnerships).

Member State responses to the GCI questionnaire are verified by the ITU GCI team. Responses are weighted based on recommendations from an expert weightage group comprised of academics, policymakers, regulators, private sector professionals, and other experts from around the globe.

National Cybersecurity Index (NCSI) - e-Governance Academy (eGA)

The National Cybersecurity Index (NCSI) provides an overview of current issues affecting the cyber realm not only in Estonia but also worldwide.[44] The NCSI measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI also offers a database with publicly available evidence materials that can be used as a tool for national cybersecurity capacity-building. Targeted at country ministries and agencies, policymakers, academia, cybersecurity experts, and any interested individual, the NCSI aims to develop a national cybersecurity assessment methodology and implement it in a country. Topics covered in the NCSI include:

1. **Cybersecurity Policy Development** (Cybersecurity Policy Unit, Cybersecurity Policy Coordination Format, Cybersecurity Strategy, Cybersecurity Strategy Implementation Plan);
2. **Cyber Threat Analysis and Information** (Cyber Threats Analysis Unit, Public Cyber Threat Reports are Published Annually, Cyber Safety and Security Website);
3. **Education and Professional Development** (Cyber Safety Competencies in Primary or Secondary Education, Bachelor's Level Cybersecurity Program, Master's Level Cybersecurity Program, PhD Level Cybersecurity Program, Cybersecurity Professional Association);
4. **Contribution to Global Cybersecurity** (Convention on Cybercrime, Representation in International Cooperation Formats, International Cybersecurity Organization hosted by the Country, Cybersecurity Capacity Building for other Countries);
5. **Protection of Digital Services** (Cybersecurity Responsibility for Digital Service Providers, Cybersecurity Standard for the Public Sector, Competent Supervisory Authority);
6. **Protection of Essential Services** (Operators of Essential Services are Identified, Cybersecurity Requirements for Operators of Essential Services, Competent Supervisory Authority, Regular Monitoring of Security Measures);
7. **E-Identification and Trust Services** (Unique Persistent Identifier, Requirements for Cryptosystems, Electronic Identification, Electronic Signature, Timestamping, Electronic Registered Delivery Service, Competent Supervisory Authority);
8. **Protection of Personal Data** (Personal Data Protection Legislation, Personal Data Protection Authority);
9. **Cyber Incidents Response** (Cyber Incidents Response Unit, Reporting Responsibility, Single Point of Contact for International Coordination);
10. **Cyber Crisis Management** (Cyber Crisis Management Plan, National-Level Cyber Crisis Management Exercise, Participation in International Cyber Crisis Exercises, Operational Support of Volunteers in Cyber Crises);
11. **Fight Against Cybercrime** (Cybercrimes are Criminalized, Cybercrime Unit, Digital Forensics Unit, 24/7 Contact Point for International Cybercrime); and
12. **Military Cyber Operations** (Cyber Operations Unit, Cyber Operations Exercise, Participation in International Cyber Exercises).

The methodology used for creating the index is described in detail on their website.[45] The index is built on data collected from three sources, the country's government officials, organizations, or individuals, and data collection by the NCSI team.

When data collection is complete, the provided information is reviewed by at least two NCSI experts. After inspection, the dataset is published on the NCSI website. Data collection, review, and publication is a continuous process, and annual iterations are not published. When new evidence is provided, the NCSI team assesses the results and, if it is grounded, makes the necessary changes in the ranking list.

National Cybersecurity Strategies Evaluation Tool – ENISA

The European Union Agency for Cybersecurity (ENISA) created a National Cybersecurity Strategies Evaluation Tool to help member states evaluate their strategic priorities and objectives related to NCSs. Through a 30-minute online evaluation, the interested country defines cybersecurity priorities and answers a few simple yes-or-no questions to receive ideas and advice for improvement. The questionnaire is sectioned into fifteen objectives:

- Objective 1: Develop national cyber contingency plans (17 questions)
- Objective 2: Protect critical information infrastructure (11 questions)
- Objective 3: Organize cybersecurity exercises (9 questions)
- Objective 4: Establish baseline security measures (13 questions)
- Objective 5: Establish incident reporting mechanisms (8 questions)
- Objective 6: Raise user awareness (8 questions)
- Objective 7: Foster R&D (16 questions)
- Objective 8: Strengthen training and educational programs (9 questions)
- Objective 9: Establish an incident response capability 5 questions)
- Objective 10: Address cybercrime (13 questions)
- Objective 11: Engage in international cooperation (not only with EU member states) (9 questions)
- Objective 12: Establish a public-private partnership (8 questions)
- Objective 13: Balance security with privacy (4 questions)
- Objective 14: Institutionalize cooperation between public agencies (5 questions)
- Objective 15: Provide incentives for the private sector to invest in security measures (7 questions)

The remarkable value of this tool is that it contemplates broad aspects that a country must take into account and that are applicable to its national context, regardless of the specific requirements of the European Union.

National Cybersecurity Framework Manual

While not a specific tool, it is important to highlight the *National Cybersecurity Framework Manual*, in which Alexander Klimburg describes five "national cybersecurity dilemmas." These dilemmas are ones that nations have to deal with in defining a strategic goal to achieve a safe and secure environment, fulfill their economic potential, and protect citizens from various cyber and non-cyber-related risks. These are:

1. **Stimulate the Economy vs. Improve National Security:** Refers to the tension existent between the expedition of the economic benefits of ICT and the Internet, while, at the same time, protecting intellectual property and privacy (data protection), securing critical infrastructure, and providing defense of the homeland.
2. **Infrastructure Modernization vs. Critical Infrastructure Protection:** Dilemma between driving infrastructure modernization (economic stimulus) and protecting critical infrastructures. Gaining efficiency and productivity can perhaps lead to the expense of basic security.
3. **Private Sector vs. Public Sector:** Governments have a clear interest in assisting the private sector in protecting the nation's essential services, wealth, and growth potential from malicious activities, but the ways and means of this assistance are fiercely debated. What is clear is that cybersecurity is a shared responsibility.
4. **Data Protection vs. Information Sharing:** Tension existing between data protection and preserving privacy and the need to share information across boundaries and borders with the intent to enhance security. National laws may be insufficient, on their own, to provide citizens with privacy protections across borders while at the same time allowing for the timely exchange of threat information.
5. **Freedom of Expression vs. Political Stability:** New technologies are being used to change the outcomes in the struggle for freedom and progress. The Internet can be co-opted as a tool to target and silence citizens. It can also be used to deny access to and use of key applications.

GUIDES

The very interconnectedness that people around the globe enjoy because of improvements in ICT can be swiftly denied, and freedom of communication and political freedom are clearly linked.

These considerations are provided here to highlight to nations that the approach they take to their cybersecurity strategy must be based on a need and must be balanced with national priorities.

Having assessed the national cybersecurity landscape, there are also various models and guides for how to develop an NCS. Some of the most well-known ones include:

- *Guide to Developing a National Cybersecurity Strategy, 2nd Edition*, by a multistakeholder group of partners[47];
- *National Cybersecurity Strategy Good Practices Guide*, by The European Union Agency for Network and Information Security (ENISA); [48]
- Commonwealth Approach for Developing National Cybersecurity Strategies, by The Commonwealth Telecommunications Organisation's ;[49]
- *Developing a National Cybersecurity Strategy*, by Microsoft;[50] and
- Catalog of project options for the National Cybersecurity Strategy (NCS) cycle, by the Global Forum on Cyber Expertise (GFCE) Strategy & Assessments Task Force.[51]

Guide to Developing a National Cybersecurity Strategy

One of the most recent guides, the 2nd edition to the *Guide to Developing a National Cybersecurity Strategy*, was developed by a group of 18 partners and 5 observers.
Version 2 of the Guide (which updates, refines, clarifies, and expands on Version 1 which was published in 2018), aims to guide national leaders and policymakers in the development of a National Cybersecurity Strategy, and in thinking strategically about cybersecurity, cyber-preparedness and resilience. It aims to provide a useful, flexible and user-friendly framework to set the context of a country's socio-economic vision and current security posture and to assist policymakers in the development of a Strategy that takes into consideration a country's specific situation, cultural and societal values, and that encourages the pursuit of secure, resilient, ICT-enhanced and connected societies.

The scope of this Guide includes both the process for developing an NCS and the content that could be included. When it comes to the process of developing an NCS, the Guide outlines the lifecycle of an NCS, including initiation, stocktaking and analysis, production, implementation, and monitoring and evaluation. Regarding content, the Guide outlines focus areas and elements that should be included in an NCS, such as:

- Governance;
- Risk management in national cybersecurity;
- Preparedness and resilience;
- Critical infrastructure and essential services;
- Capability and capacity building and awareness-raising;
- Legislation and regulation; and
- International cooperation.

In addition, the Guide outlines cross-cutting considerations to be considered during the development of an NCS, including:

- vision;
- comprehensive approach and tailored priorities;
- inclusiveness;
- economic and social prosperity;
- fundamental human rights;
- risk management and resilience;
- appropriate set of policy instruments;
- clear leadership,
- roles, and resource allocation;
- trust environment.

National Cybersecurity Strategy Good Practice Guide - The European Union Agency for Network and Information Security (ENISA)

The European Union Agency for Cybersecurity, ENISA, is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.

ENISA published its first *National Cyber Security Strategies* paper in 2012.[52] Since then, EU Member States and EFTA countries have made progress in developing and implementing their strategies. They published a revised Guide in 2016 which updates the different steps, objectives, and good practices of the original guide and analyses the status of NCS in the European Union and EFTA area. The aim of the *NCS Good Practice Guide* is to support EU Member States in their efforts to develop and update their NCS. Despite the main target audience being public officials and policymakers, the Guide could also be a useful resource to other stakeholders involved in the lifecycle of the strategy, such as private, civil and industry stakeholders.

The *NCS Good Practice Guide* outlines the NCS lifecycle, providing examples of good practice in developing, implementing, and evaluating an NCS.

ENISA has published other relevant resources, including:

- *Good practices in innovation on Cybersecurity under the NCS*;[53]
- *National Cyber Security Strategies: An Implementation Guide*;[54] and
- *An Evaluation Framework for Cyber Security Strategies*.[55]

The National Cybersecurity Strategies: An Implementation Guide may be of particular use when it comes time to evaluate the impact of an NCS (see the section on Monitoring and Evaluation below). It provides a set of concrete actions, which, if implemented, will lead to a coherent and holistic NCS. It also proposes an NCS lifecycle, with a special emphasis on the development and execution phase. For each component of the strategy, it offers a list of possible and indicative key performance indicators (KPIs).

The Guide proposes Deming's "Plan-Do-Check-Act" (PDCA) model for governing an NCS, as well as three approaches that can be pursued in governing a strategy:

- A linear approach: the strategy will be developed, implemented, evaluated, and eventually terminated (or replaced);
- A lifecycle approach: the output of the evaluation phase will be used to maintain and adjust the strategy itself; and
- A hybrid approach: several continuous improvement cycles on different levels may exist.

Commonwealth Approach for Developing National Cybersecurity Strategies - The Commonwealth Telecommunications Organisation

The Commonwealth Telecommunications Organisation (CTO) is the Commonwealth agency mandated in the field of ICT and works towards helping its members leverage ICTs for socio-economic development. Its two-tier membership facilitates consultations between Commonwealth countries, non-Commonwealth countries, industry, and civil society to arrive at harmonized approaches on ICT-related issues with global implications.

The CTO developed a *Commonwealth Approach for Developing National Cybersecurity Strategies* based on the Commonwealth Cybergovernance Model and drawing on operational Cybersecurity Strategies from several countries like Austria, Australia, Canada, France, Finland, Germany, India, The Netherlands, Spain, Switzerland, Trinidad and Tobago, Italy, the United Kingdom, and the United States, as well as NCS guides. [56]

The Guide was revised in 2015 and outlines the process to develop, deliver, and review strategies, as well as the actual elements that the strategy should include, namely:

- Introduction and background;
- Guiding principles;
- Vision and strategy;
- Objectives and priorities – using a risk-based approach;
- Stakeholder section;
- Governance and management structure;
- Strategy implementation, including legal and regulatory frameworks, capacity building, awareness, local technical capability, and incident response; and
- Monitoring and evaluation.

Developing a National Strategy for Cybersecurity - Microsoft

In 2013, Microsoft published a document containing recommendations for policymakers to develop or improve an NCS.

The document, *Developing a National Strategy for Cybersecurity: Foundations for Security, Growth and Innovation*, explains what a cybersecurity strategy is and then outlines six foundational principles as the basis for a national strategy (namely: risk-based, outcome-focused, prioritized, practicable, respectful of privacy and civil liberties, and globally relevant).[57] The report then goes on to make recommendations for the development of a strategy.

REGIONAL AND INTERNATIONAL PROGRAMS

There are many actors in the cybersecurity capacity-building space. While states retain the primary role and charge for public security (including in the realm of cyberspace), there are shortfalls in their technical, economic, and human resources that limit their ability to put adequate measures in place to protect their digital assets. This limitation extends to a state's ability to cooperate internationally in the face of a cyber-incident that may have perpetrated a cybercrime. As a result, the global community (international and regional actors) have found it necessary to coordinate cybersecurity capacity-building programs that states can access to help them develop a structured NCS. This section reviews some of these coordinating organizations and provides a brief overview of what their programs entail as of the date of writing this publication.

- CARICOM Implementation Agency for Crime and Security (CARICOM IMPACS) - 11th EDF EU Project;[58]
- Council of Europe - Global Action on Cybercrime Extended (GLACY)+; [59]
- Government of the United States- Digital Connectivity and Cybersecurity Partnership;[60]
- International Telecommunication Union;
- Organization of American States;[61]
- The Commonwealth (through the Commonwealth Telecommunications Organisation);[63]
- The Global Forum on Cyber Expertise; and
- The World Bank.[64]

In some instances, assistance is offered to countries as a part of a developed countries cybersecurity strategy for international cooperation; bi-laterals are entered into between states for assistance in specific areas of need of the receiving state. Further, some mature states have also considered this assistance as a part of their foreign assistance programs and have created specific funding for developing cybersecurity capacity in less developed nations. These project funding are usually geared towards specific outputs and often include priority nations. Traditional development organizations are an additional avenue to approach for support as they have seen the explicit link between traditional development projects such as digital and broadband initiatives and the need for this to be layered with cybersecurity considerations at the onset[65].

Finally, regional organizations also have a role to play. These bodies traditionally work with their member states to obtain consensus on common areas of interest among their member states that could have regional impact. In recent years, many organizations such as CARICOM, the OAS and others, have received specific mandates from their member states to build the cyber capacity of their member states to better address cyber threats at both the human resource and technical level.

Having identified the need and the stakeholders, a nation needs to recognize the importance of strategically managing these opportunities. They must recognize that the needs are not all mutually exclusive and that duplication, while not desirable, may be unavoidable. As Klimburg and Zylberberg state in the Cyber Security Capacity Building report,

> "[Cybersecurity Capacity Building] CCB is a recent addition to the security/development nexus. In comparison to other security and development issues, like Security Sector Reform (SSR), or Disarmament, Demobilization and Re-Integration (DDR), CCB stands out as much more connected to the broader economic landscape, with security issues that are even more immediately cross-border, and deals with overall issues that are (arguably) much more complex in width (thematic reach) and depth (technical detail)."[66]

CARICOM Implementation Agency for Crime and Security (CARICOM IMPACS) - 11th EDF EU Project

Implementer of donor funds/Regional Organization

CARICOM IMPACS commenced the execution of the 11th EDF project entitled: 'Capacity Building for CARIFORUM Member States on Asset Recovery and Cybercrime' in January 2019.[67] The

project has a lifecycle of 48 months. The overall objective of the project Capacity Development of CARIFORUM Member States on Financial Compliance, Asset Recovery and Cybercrime, is to contribute to the improvement and sustainability of safety and security in the CARIFORUM region. The project is subdivided into two areas: Asset Recovery and Cybercrime.

The cybercrime component of this project is focused on enhancing detection and investigation of cybercrimes in CARIFORUM member states in compliance with international standards. There are five intended outputs of this component:

1. Increased compliance of national legislations and policies with international standards on cybercrime (as prescribed in the Budapest Convention on Cybercrime);
2. Increased due-process compliance capacities of criminal justice authorities (police, judiciary) to investigate, prosecute, and adjudicate cases of cybercrime and electronic evidence and engage in effective inter-agency, public-private, and international cooperation;
3. Increased awareness and capacities amongst decision makers, parliamentarians, relevant national authorities including public service ICT professionals on cybercrime and cybersecurity policies;
4. Strengthened regional coordination of cybercrime/ cybersecurity activities through IMPACS as the main coordinating agency for implementing the CCSCAP, including capacity building for CARICOM IMPACS and its sub-agencies; and
5. Improved capacities of the Regional Intelligence Fusion Centre (RIFC) and National Intelligence Points of Contacts in Member States, for information gathering and strategic analysis.

Under each component, CARICOM member states will participate in several meetings and training workshops.

Council of Europe - Global Action on Cybercrime Extended (GLACY)+

Capacity building program specific to cybercrime/Regional Organization

GLACY+ is a joint project of the European Union (Instrument Contributing to Peace and Stability) and the Council of Europe.[68] According to the website, it is intended to extend the experience of the GLACY project (2013 – 2016) and supports fifteen priority and hub countries in Africa, Asia-Pacific and LAC region – Benin, Burkina Faso, Cabo Verde, Chile, Costa Rica, Dominican Republic, Ghana, Mauritius, Morocco, Nigeria, Paraguay, Philippines, Senegal, Sri Lanka, and Tonga. These countries may serve as hubs to share their experience within their respective regions.

The objectives of GLACY+ are:

1. To strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area;
2. To promote consistent cybercrime legislation, policies, and strategies;
3. To strengthen the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions; and
4. To enable criminal justice authorities to apply legislation, prosecute, and adjudicate cybercrime cases, and electronic evidence and engage in international cooperation.

The priority countries have the ability to approach the Council of Europe to request cooperation through their Global Action on Cybercrime Extended (GLACY+) Program to implement a cybercrime act that can enable those countries to adhere to the Budapest Convention. This will enable them to exchange information and build capacities with other members more efficiently. Once that country has implemented the recommendations and developed a cybercrime act that aligns with the Budapest Convention, they may be invited officially to adhere to the convention.

Government of the United States - Digital Connectivity and Cybersecurity Partnership

Developed good practice guidance through MITRE for assessment and provides capacity building in-kind and as a donor/Donor State

The Digital Connectivity and Cybersecurity Partnership ('Digital Partnership' or DCCP) is a multi-year, whole-of-government effort to promote an open, interoperable, secure, and reliable Internet.[69] By catalyzing economically sustainable and secure private sector network investments and promoting regulatory reforms and adoption of cybersecurity best practices, this initiative will provide a credible alternative to top-down, authoritarian approaches to Internet and ICT development and enable nations to realize the tremendous economic benefit of the digital economy.

The DCCP starts with a $25 million initial investment to improve partner countries' digital connectivity and expand opportunities for US technology exports. The United States will support communications infrastructure development through technical assistance and public-private partnerships; promote market-driven digital regulatory policies; and build partners' cybersecurity capacity to address common threats.

Through the United States Department of State, MITRE also works with the government to build cyber policies and strategies in developing nations. The MITRE team provides the thinking and tools to assist a national government in building secure, open, and more resilient cyber ecosystems.[70] In 2016, they developed the *National Cyber Strategy Development & Implementation (NCSDI) Framework* for building cyber capacity. This framework addresses the building blocks of cyber capacity based on eight key capability areas. It continues to be a living and evolving process. They have also directly supported US missions in five developing countries and worked at varying levels with international organizations such as the Economic Community of West African States, the Organization for Security and Cooperation in Europe, and the OAS—reaching more than 100 nations.

International Telecommunication Union (ITU-D) Cybersecurity Program

Developed an assessment tool, good practice guide and offers capacity building/Regional Organization

According to ITU, cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.

The Cybersecurity Program offers ITU members – particularly developing countries – the opportunity and tools to increase cybersecurity capabilities at the national level, enhance security, and build confidence and trust in the use of ICTs, thus making the digital realm more safe and secure for everyone.[71] The work and mandate of the cybersecurity program builds on Objective 2 of the Buenos Aires Action Plan adopted at the 2017 World Telecommunication Development Conference, and related resolutions.[72]

According to ITU, adopting and implementing an NCS can be particularly challenging for developing countries as it requires significant economic, human, and organizational resources. In an effort to ease that burden, the ITU has published resources to develop NCSs and assisted their member states in the development of their own NCS. The ITU also offers NCS virtual training. This training, based on the Guide, is free and open. It is available in English, French, Spanish, and Russian.

Recently, the ITU used the Bhutan case study to highlight that developing the NCS spread cybersecurity awareness and visibility throughout the institutional apparatus. The new strategy development was informed by the first edition of the *National Cybersecurity Strategy Guide*, and in consultation with national key stakeholders.[74] The high-level ICT steering committee in Bhutan, with members representing top management from every sector (government, public and private), drives and monitors the implementation of ICT projects. In terms of funding, Bhutan's Department of IT & Telecom secured a dedicated budget projected over five years to implement the NCS. The ITU has indicated that to date, they have supported more than 30 countries with drafting and implementing national cybersecurity strategies and assessed over 80 countries' readiness to embark on the development of national computer incident response teams.[75]

Organization of American States

Implements the CMM, develops good practice guides and offers capacity building but does not generate its own funding or provide funding. Technical assistance is in-kind or as an implementer of donor funds.

The OAS's Cybersecurity Program implements technical assistance projects with the support of specific funds from various donors, including private sector, member states, development entities, and observer nations.[76] The overall objective of the Cybersecurity Program is to improve member states' capabilities to detect cyber threats, prevent, respond to and recover from cyber incidents, and prevent cybercrime, based on a multistakeholder engagement approach. As a part of these technical assistance programs, the OAS executes technical missions to assess member states' cybersecurity preparedness and the development of their national cybersecurity strategies. The OAS has promoted stakeholder roundtables and moderated working groups intending to identify member states' cybersecurity issues and develop solutions oriented to the country's realities. The OAS provides technical writing support and produces reports summarizing the findings from the meetings; recommendations are made on concrete actions that member states' governments can undertake. The information also informs the development of an NCS and often highlights key actors that should play a role in implementing strategic actions to improve a country's cybersecurity capability.

The OAS also leverages the expertise of international experts in the field of cybersecurity. These experts participate in the roundtable discussions and provide input and recommendations based on an assessment of the information gathered during the meetings. The recommendations address international frameworks, responses to cybersecurity incidents, investigative tools, and legislation necessary to address cybercrime, cyber defense, and international cooperation. These recommendations are prepared closed-door among the experts and guaranteed by confidentiality and impartial analysis.

The Commonwealth (through the Commonwealth Telecommunications Organisation)

Developed political policies and provides capacity building in-kind and as a donor/Regional Organization

According to the Commonwealth, the world is witnessing the emergence of contrasting views and approaches on how to govern cyberspace. Mindful of the unique nature of cyberspace and of the importance of maintaining it as a place that fosters interactions, innovation, and entrepreneurship, the CTO embarked on a project to develop the Commonwealth Cybergovernance Model that draws on the shared values and principles of the Commonwealth as encompassed in the Commonwealth Charter.[77] The Commonwealth ICT ministers adopted the Commonwealth Cybergovernance Model at the meeting held in London in March 2014. The CTO developed a *Commonwealth Approach for Developing National Cybersecurity Strategies based on the Commonwealth Cybergovernance Model.*[78] In the coming years, the CTO will work with its member countries, member institutions, and partner organizations to convert the Cybergovernance Model into practical actions and to implement NCSs, so that cyberspace and ICTs of all forms are safe, secure, and resilient.

The Global Forum on Cyber Expertise

Catalog of project options for the National Cybersecurity Strategy (NCS) cycle - GFCE Task Force on Strategies and Assessments

The GFCE's Catalog aims to inform countries of the types of support activities available from GFCE Members and Partners, and to help program managers design projects.[79] It offers examples of 20 activities that could go into a project supporting a country's NCS cycle, such as conducting a national incident response capacity review, gathering data on cybersecurity vulnerabilities, offering advice on how to include stakeholders in an inclusive strategy development process, and offering advice from experts on strengthening cross-government coordination, among other activities.

The GFCE's Catalog aims to inform countries of the types of support activities available from GFCE Members and Partners, and to help program managers design projects. It offers examples of 20 activities that could go into a project supporting a country's NCS cycle, such as conducting a national incident response capacity review, gathering data on cybersecurity

vulnerabilities, offering advice on how to include stakeholders in an inclusive strategy development process, and offering advice from experts on strengthening cross-government coordination, among other activities.

The World Bank

Provides capacity building as a loan and as a donor through grants/Development Organization

In this context, The World Bank has taken both the role as a lender and as a facilitator for capacity building. The World Bank's new Digital Development Partnership (DDP) helped to operationalize the 2016 *World Development Report on Digital Dividends* and offers a platform for digital innovation and development financing.[79] The DDP brings public and private sector partners together to catalyze support to developing countries in the articulation and implementation of digital development strategies and plans. This partnership makes digital solutions available to developing countries with an emphasis on the following areas:

- Data and indicators;
- Digital economy enabling environment;
- **Cybersecurity;**
- Internet access for all;
- Digital government; and
- Mainstreaming digital services, solutions, and platforms.

Under cybersecurity, concerns grow in parallel with the adoption of digital services and infrastructure. DDP helped the capacity of The World Bank's clients in the development of cybersecurity policies and standards and supported good practices in the use of cybersecurity tools, safeguards, and risk management instruments.

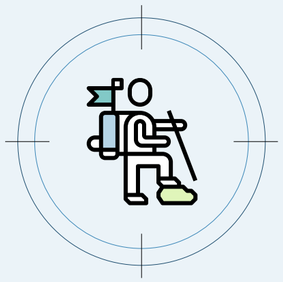
According to The World Bank, the fourth Industrial Revolution is unfolding at full speed and is prompting governments to optimize current IT systems by adopting new technologies for the re-engineering of processes, as well as to provide new public services. Cloud computing, artificial intelligence, big data analytics, and new technologies are changing the modus operandi of the government systems in charge of public finance management, human resources, and government service delivery. As "going digital" helps increase efficiency and reduce costs, other government systems are also likely to follow suit. Recognizing the potential risks associated with going digital, the Global Cybersecurity Capacity Program was established under the Korea-World Bank Group Partnership (KWPF) between 2016 and 2019. Its implementation was structured into four main elements:

i. Identification of the beneficiary countries and program setup;
ii. Gap analysis and identification of cybersecurity priorities, and dissemination of results;
iii. Delivery of capacity building and/or technical assistance based on the results of element 2; and
iv. Activity impact assessment.

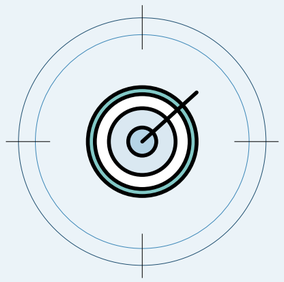
This project was focused on tailored specific national and regional technical assistance schemes and was *"an attempt to bridge existing gaps in cybersecurity capacities, especially in the case of governments that have taken out loans from WB to cover the needs of their emerging digital economies."*[81] According to the Lessons Learned report, each of the beneficiary countries underwent a CMM assessment conducted by the creator of the CMM, the GCSCC. Following the CMM exercise and delivery of analytical reports, another strategic partner on the Program—the Global Cybersecurity Center for Development (GCCD) under Korea Internet and Security Agency (KISA)—delivered a series of in-country cybersecurity capacity-building workshops. Finally, a selected set of countries received country-specific or regional technical assistance in the form of analytical studies and inputs related to cybersecurity. What is noticeable from the report is that The World Bank meets their client's needs for cybersecurity through financing and analytical and advisory support.[82]

Figure 3 **General Goals of a Cybersecurity Program**[83]

General Aspects From its outset, the Program pursued the following key objectives:

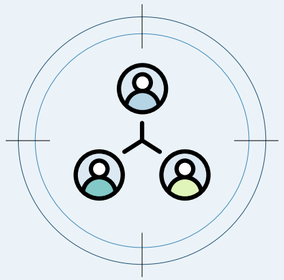


Improve beneficiary countries' understanding of cybersecurity maturity status quo, existing gaps, and priorities at the national level.



Improve beneficiary countries' awareness and capacity to identify and engage with relevant stakeholders at the national level in the context of cybersecurity.

Strengthen beneficiary countries' capacity in at least one of the identified priorities (GAP) and broaden client understanding on how to move ahead with other priorities (GAPS)



Perform a donor coordination effort at the national level, map cybersecurity activities undertaken by different donors, and secure synergies.

More recently, on 22 June 22 2020, The World Bank approved the Caribbean Digital Transformation Project, for a total of US$94 million for four Eastern Caribbean countries: Dominica (US$28 million), Grenada (US$8 million), Saint Lucia (US$20 million), Saint Vincent and the Grenadines (US$30 million), and the Organization of Eastern Caribbean States (OECS) Commission (US$8 million) to build an inclusive digital economy. This is the first World Bank-financed project to support the development of the digital economy in the Caribbean. It aims to increase access to digital services, technologies, and skills by governments, businesses, and individuals. The project aims to increase Internet penetration and access to digital financial services and public services. It will support reforms and regional harmonization of the legal and regulatory environment to promote investment in digital infrastructure. It will support activities to make telecommunications and financial services more affordable, while addressing risks related to cybersecurity and data protection. The project will also support public sector modernization and delivery of citizen-centric, digital public services. Support will be provided to individuals and businesses for skills and entrepreneurship development.

The World Bank example offers insight into the convergence of the 'why' (SDG), the 'how' to start (CMM tool), and the 'how' to implement (capacity building workshops).

GLOBAL CYBER CAPACITY-BUILDING PROGRAMS

With that said, member states on this journey don't need to go it alone. There are different approaches to states receiving external assistance to determine the 'how' to develop and implement. Building cybersecurity capacity should go hand-in-hand with building an NCS.

According to New America Foundation,

> "These donors wield influence through carrots, like the promise of more money as a reward for good practice, and sticks, like loan cancellations and loan conditions. While donors most often work with recipients of the investment or loan to tailor a project or program to fit the recipients' needs, donors do, nonetheless, have a great deal of agenda-setting and steering power. For this reason, generating greater understanding of the importance of cybersecurity to safeguard and enable the investments of the donor community is crucial."[84]

As stated by New America, *"the donor community's reliance on metrics to steer investment means that the cybersecurity capacity-building community will need to create an empirically convincing argument that an absence of better cybersecurity leads to demonstrably worse outcomes."* Extrapolating from that position, the conclusion is that states must align their assessment, prioritization, and funding in order to be successful. We set out below the 'how' to disaggregate this various assistance to ensure it aligns with member states' own national goals.

Cyberspace is an intrinsic part of the development of any country. A mature national cyber capacity is crucial for states to progress and develop economically, politically, and socially. The cyber community, academia, and policymakers have documented the need to integrate cyber capacity-building and development policies. The investment in securing cyberspace affects the success rate of other policy initiatives as well. However, there is a clear need for a deeper dialogue with the development community and recipient countries in order to better understand how to implement cyber capacities to achieve broader development goals.[85] These programs are crucial to further cyber capacity building, and whilst it's outside of the scope of the document to provide a more detailed overview, there are resources that readers might find useful, such as the Cybil Portal, a knowledge portal for cyber capacity building which provides information on over 800 cyber capacity building projects, and 745 relevant actors.

The need for a contextualized roadmap

Whichever approach a country chooses to follow, the roadmap they develop must respond to the specific context, needs, and goals of the country and its processes. To be as effective as possible, NCSs and, more broadly, cyber policies and capacity-building efforts, should be targeted and tailored to the specific threat and opportunity context of a country. There is no one-size-fits-all solution to cybersecurity. While the use of templates or "premade" tools offer a good starting point, they cannot take into account the nuances of the cyber landscape on the ground. These templates are also likely to miss some key consultative processes that would support the creation of trust and identification of human rights considerations and cultural and political context that can impact the implementation of a cybersecurity strategy or policy.

When putting together a roadmap for NCS development, a country could review the different existing guides on the topic of NCS development, identify which elements could be useful for their specific context, and create a process that is tailored to their concrete needs.

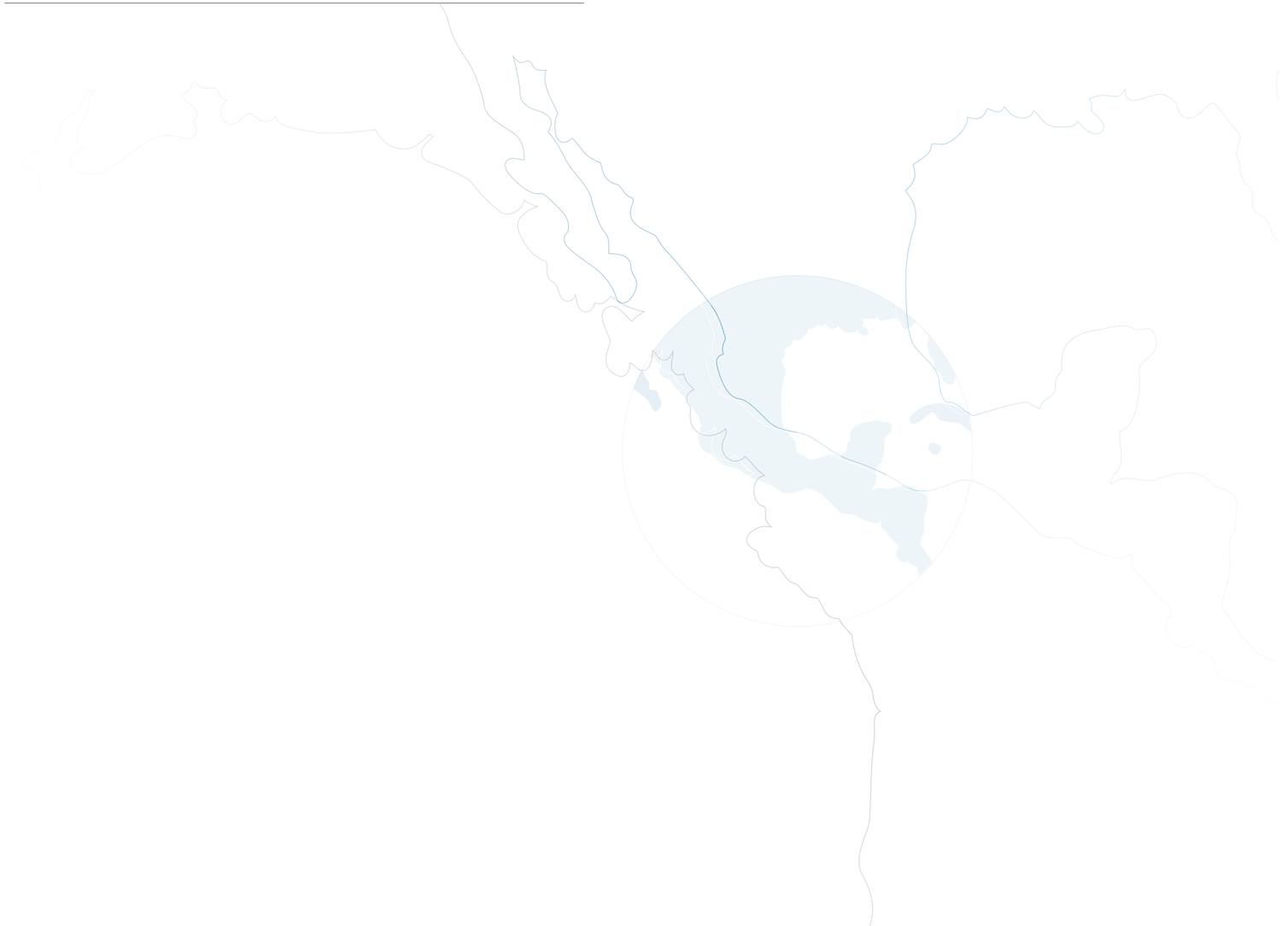
STRATEGY DEVELOPMENT BASED ON ASSESSMENT RESULTS

Once the assessment phase is completed, at the national level, a state now has to consider the 'what' to include in the NCS. The assessment phase will highlight many gaps and strengths in one's national cyber capability, and it is critical to determine what should be tackled as a priority. As mentioned previously, nations have to deal with several national cybersecurity dilemmas when defining their strategic goals to achieve a safe and secure environment that fulfills their economic potential and protects citizens from various cyber and non-cyber related risks.[86] Two of these are particularly relevant:

1. **Stimulate the Economy vs. Improve National Security:** Refers to the tension existent between the expedition of the economic benefits of ICT and the Internet, while, at the same time, protecting intellectual property and privacy (data protection), securing critical infrastructure, and providing defense of the homeland.

2. **Infrastructure Modernization vs. Critical Infrastructure Protection:** Dilemma between driving infrastructure modernization (economic stimulus) and protecting critical infrastructures. Gaining efficiency and productivity can perhaps lead to the expense of basic security.

The decision of what to include in the NCS should be based on the results of the assessment and then link this to the motivation (which was elaborated in Part 1). In ranking the priority, motivation becomes key as this will often indicate where resources are located and how they will be allocated to meet the objectives of the NCS.



Notes

30 Deborah Bodeau, and Richard Graubart, "Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness," (MITRE, 2017), Project No.: 01ADM105-CP, Department No: J83C, https://www.mitre.org/sites/default/files/publications/16-0939-motivating-organizational-cyber-strategies.pdf.

31 For a full overview of existing assessment tools, refer to the "Global Forum on Cyber Expertise's Global Overview of Existing National Cyber Capacity Assessment Tools," Cybil Portal, accessed April 21, 2022, https://cybilportal.org/publications/global-overview-of-assessment-tools-goat/.

32 The World Bank and the United Nations, Combatting Cybercrime: Tools and Capacity Building for Emerging Economies, (Washington, D.C., 2017), https://www.combattingcybercrime.org/.

33 Melissa Hathaway (Principal Investigator), Cyber Readiness Index 2.0 - A Plan for Cyber Readiness: A Baseline and an Index, (Potomac Institute for Policy Studies, 2015), https://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

34 "Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 edition," Global Cyber Security Capacity Centre (GCSCC), University of Oxford, accessed April 21, 2022, https://gcscc.ox.ac.uk/the-cmm#/.

35 "Global Cybersecurity Index," International Telecommunications Union (ITU), accessed April 21, 2022, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

36 "National Cyber Security Index," E-Governance Academy (EGA), accessed April 21, 2022, https://ncsi.ega.ee.

37 "National Cybersecurity Strategies Evaluation Tool," European Union Agency for Cybersecurity (ENISA), accessed April 21, 2022, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

38 Alexander Klimburg, National Cybersecurity Framework Manual, (NATO CCD COE Publications, 2012), https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

39 The World Bank and the United Nations, Combatting Cybercrime: Tools and Capacity Building for Emerging Economies.

40 Melissa Hathaway (Principal Investigator), Cyber Readiness Index 2.0 - A Plan for Cyber Readiness

41 Melissa Hathaway, "The Future of Cybersecurity with Melissa Hathaway," Potomac Institute for Policy Studies, accessed April 21, 2022, https://www.potomacinstitute.org/divisions/34-science-and-technology-policy/cyber-readiness/cyber-readiness-news/92-the-future-of-cybersecurity-with-melissa-hathaway.

42 "Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 edition," https://gcscc.ox.ac.uk/the-cmm#/.

43 "Global Cybersecurity Index," https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

44 "National Cyber Security Index," https://ncsi.ega.ee.

45 Ibid.

46 "National Cybersecurity Strategies Evaluation Tool," https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

47 Council of Europe (CoE), Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organization (INTERPOL), International Telecommunication Union (ITU), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations University (UNU), Guide to Developing a National Cybersecurity Strategy 2nd Edition – Strategic engagement in cybersecurity, (2021), Creative Commons Attribution-NonCommercial 3.0 IGO (CC BY-NC 3.0 IGO), https://ncsguide.org/the-guide/.

48 ENISA, NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies, (ENISA, 2016), https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

49 Commonwealth Telecommunications Organisation (CTO), Commonwealth Approach for Developing National Cybersecurity Strategies, (CTO, 2015), https://www.cto.int/strategic-goals/cybersecurity/national-strategies/.

50 Microsoft, Developing a National Strategy for Cybersecurity, (Microsoft, 2013),https://www.microsoft.com/en-us/cybersecurity/content-hub/developing-national-strategy-for-cybersecurity.

51 "Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle," Cybil Portal, accessed April 21, 2022, https://cybilportal.org/publications/catalog-of-project-options-for-the-national-cybersecurity-strategy-ncs-cycle/.

52 ENISA, National Cyber Security Strategies, (ENISA, 2012), https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.

53 ENISA, Good practices in innovation on Cybersecurity under the NCSS, (ENISA, 2019), https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.

54 ENISA, National Cyber Security Strategies: An Implementation Guide, (ENISA, 2012), https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

55 ENISA, An evaluation framework for Cyber Security Strategies, (ENISA, 2014), https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.

56 "Cybersecurity Strategy List of Reading", Commonwealth Telecommunications Organisation (CTO), accessed April 21, 2022, https://cto.int/strategic-goals/cybersecurity/national-strategies/.

57 Developing a National Strategy for Cybersecurity, https://www.microsoft.com/en-us/cybersecurity/content-hub/developing-national-strategy-for-cybersecurity.

58), "11th EDF Tender to Supply and Install Digital Forensic Management Platform Hardware and Software," Caribbean Community Implementation Agency for Crime and Security (CARICOM IMPACS), accessed August 31, 2021, https://caricomimpacs.org/11th-edf-project/

59 "Global Action on Cybercrime Extended (GLACY)+," Council of Europe, accessed August 31, 2021, https://www.coe.int/en/web/cybercrime/glacyplus.

60 "Digital Connectivity and Cybersecurity Partnership," US Department of State, Division for International Communications and Information Policy, accessed on April 21, 2022, https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/.

61 "Cybersecurity Program," Organization of American States, accessed April 22, 2022, https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp.

62 "Cybersecurity," Commonwealth Telecommunications Organisation (CTO), accessed September 1, 2021, https://cto.int/strategic-goals/cybersecurity/.

63 "Global Forum on Cyber Expertise (GFCE)", GFCE, accessed April 22, 2022, https://thegfce.org/.

64 World Bank Group, Global Cybersecurity Capacity Program: Lessons Learned and Recommendations towards Strengthening the Program, (The World Bank, 2019), https://documents.worldbank.org/en/publication/documents-reports/documentdetail/947551561459590661/global-cybersecurity-capacity-program-lessons-learned-and-recommendations-towards-strengthening-the-program.

65 To read more about the links between the development and cyber capacity building communities, see Robert Collett and Nayia Barmpaliou , International Cyber Capacity Building: Global Trends and Scenarios, European Union Institute for Security Studies, (Luxembourg, Publications Office of the European Union, 2021), p 38, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf. and Melissa Hathaway and Francesca Spidalieri, Integrating Cyber Capacity into the Digital Development Agenda, (GFCE Foundation, 2021), https://thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf.

66 Alexander Klimburg and Hugo Zylberberg, Cyber Security Capacity Building: Developing Access, (Norwegian Institute of International Affairs, 2015), https://www.nupi.no/en/Publications/CRIStin-Pub/Cyber-Security-

Capacity-Building-Developing-Access.

67 11th EDF Tender to Supply and Install Digital Forensic Management Platform Hardware and Software," https://caricomimpacs.org/11th-edf-project/.

68 "Global Action on Cybercrime Extended (GLACY)+," https://www.coe.int/en/web/cybercrime/glacyplus.

69 "Digital Connectivity and Cybersecurity Partnership," https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/.

70 MITRE, "MITRE Strengthens Cyber Capacity of Developing Nations," MITRE, December, 2019, https://www.mitre.org/publications/project-stories/mitre-strengthens-cyber-capacity-of-developing-nations.

71 "ITU-D Cybersecurity," International Telecommunications Union Cybersecurity Program, accessed April 22, 2022, https://www.itu.int/itu-d/sites/cybersecurity/.

72 ITU, "World Telecommunication Development Conference (WTDC-17) Buenos Aires, Argentina, 9-20 October 2017, Final Report," (ITU, 2018), p 49, https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17_final_report_en.pdf.

73 Bhutan Computer Incident Response Team (BtCIRT), "What we learned while developing Bhutan's first National Cybersecurity Strategy," MyITU, November 22, 2021, https://www.itu.int/en/myitu/News/2020/11/05/08/52/Bhutan-first-National-Cybersecurity-Strategy-BtCIRT.

74 "National Strategies," International Telecommunications Union, accessed April 22, 2022, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.

75 Malcom Johnson, "Here's how we can strengthen cybersecurity for 'the New Normal'" MyITU, November 26, 2020, https://www.itu.int/en/myitu/News/2020/11/25/16/59/Stronger-cybersecurity-new-normal-Malcolm-Johnson.

76 "Cybersecurity Program," https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp.

77 Commonwealth ICT Ministers Forum 2014, Marlborough House, London, Commonwealth Cybergovernance Model, 3-4 March 2014, available at: https://www.cto.int/wp-content/uploads/2021/09/The-Commonwealth-Cybergovernance-Model.pdf.

78 Commonwealth Approach for Developing National Cybersecurity Strategies, https://www.cto.int/strategic-goals/cybersecurity/national-strategies/.

79 Global Forum on Cyber Expertise, "Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle", GFCE, last modified June 10, 2021, https://cybilportal.org/wp-content/uploads/2021/06/GFCE-catalog-of-project-options-NCS_edited10June.pdf.

80 The World Bank, World Development Report 2016: Digital Dividends, (World Bank, 2016), https://www.worldbank.org/en/publication/wdr2016.

81 Global Cybersecurity Capacity Program: Lessons Learned and Recommendations towards Strengthening the Program, 4, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/947551561459590661/global-cybersecurity-capacity-program-lessons-learned-and-recommendations-towards-strengthening-the-program.

82 Ibid, 6.

83 Ibid. Figure by The World Bank and used with permission.

84 National Cybersecurity Framework Manual, https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

85 To read more about the links between the development and cyber capacity building communities, see Collett and Barmpaliou, International Cyber Capacity Building: Global Trends and Scenarios, p 38; and Hathaway and Spidalieri, Integrating Cyber Capacity into the Digital Development Agenda. See also Lilly Pijnenburg Muller, Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities, (Norwegian Institute of International Affairs Report no 3, 2015), https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/284124/NUPI%2bReport%2b03-15-Muller.pdf?sequence=3&isAllowed=y.

Part **4**

PRACTICAL APPROACHES - ROADMAPS AND IMPLEMENTATION

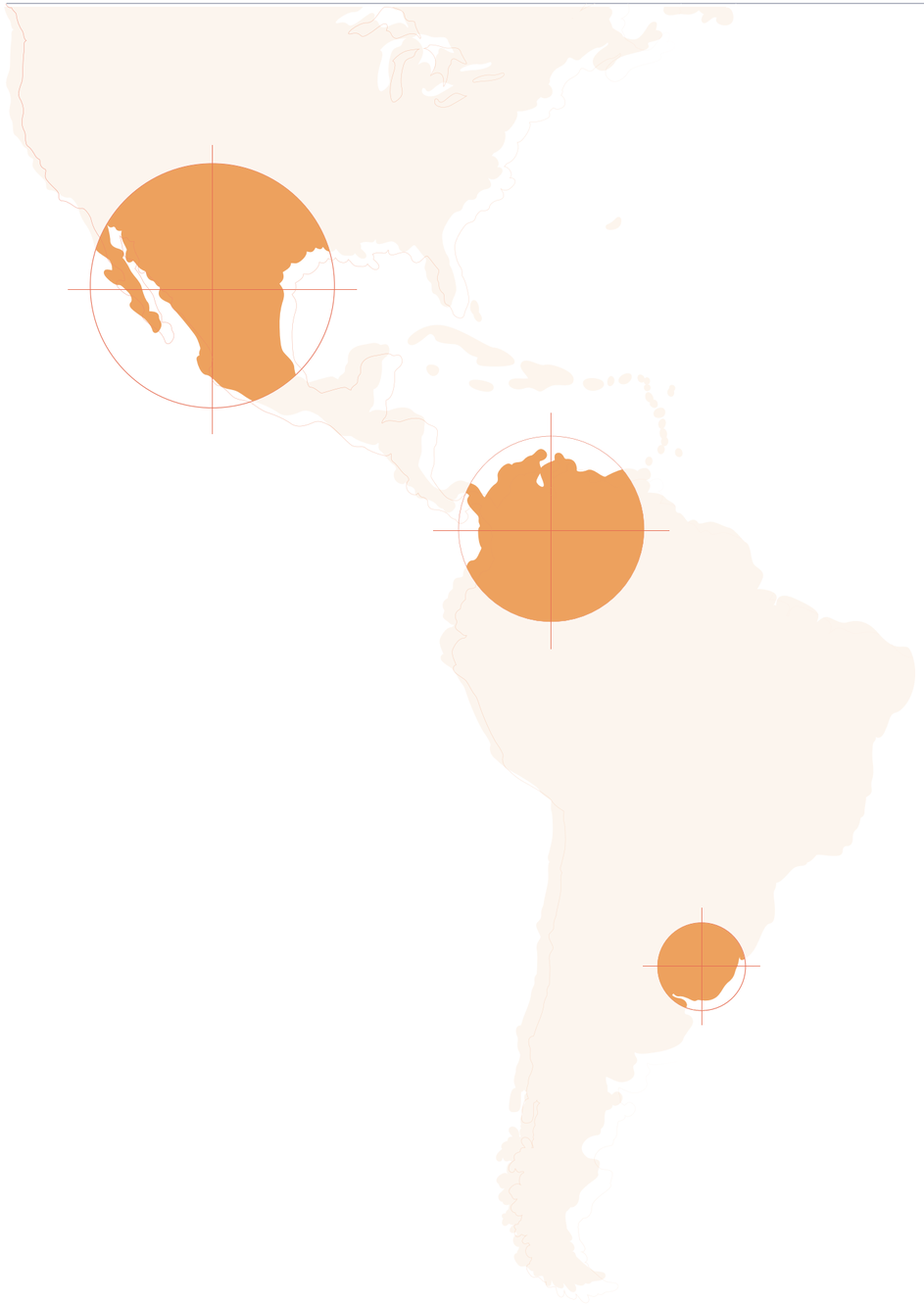
The previous sections offered guidance on tools and guides that exist to help develop an NCS. This section focuses on the implementation stage for an NCS by exploring the process of organizing and prioritizing. It also explores considerations to ensure sustainable implementation, monitoring, and evaluation, including different existing monitoring and evaluation frameworks, mechanisms to keep targets on track, and regional examples.

Our aim for this section is not to re-state or summarize what has been outlined in the guides described in Part 3 but to instead build on existing good practices by highlighting practical approaches taken by donor nations, development organizations, and regional bodies who have been offering technical assistance globally to states in the area of policy/strategy development.

In general, countries will first perform an assessment to determine where they must focus their energies, then move into implementation. However, it is not uncommon to kick off an implementation process by selecting an assessment tool or guide and using it to guide the effort. The utilization of an assessment tool at the beginning must come with some background knowledge of where to begin. Many technocrats charged with the responsibility to develop a national-level policy or strategy are often struck by the reality that they have a general idea of what is needed but are not sure how to go about doing it. The choice between whether to separate the assessment process from the implementation process is determined by the needs and priorities of each government. This section assumes that a strategic planning committee has completed the NCS, and the implementation committee is taking the next steps.

Implementation Plans in Colombia, Mexico, and Uruguay

In Colombia, an annex was included in the NCS in which the Action and Follow-up Plan (PAS) was established for the timeframe of 2020-2022. The PAS set out the actions to be developed by each of the different entities involved in the document to achieve the policy objectives. Each action has indicators, a presumed budget, and milestones for its fulfillment, allowing for the measurement of project goals in the execution of the action and financial progress. Additionally, there is a monitoring platform for each action, where the competent entities have to report the progress along with supporting evidence. The strategy is monitored based on the reports presented by the National Planning Department within the framework of the Digital Security Committee, which is responsible for the inter-institutional articulation of the public entities in charge of security and digital defense.
In Mexico, in October 2017, an agreement was adopted for the creation of the Cybersecurity Subcommittee, chaired by the Ministry of the Interior through the National Security Commission and its Scientific Division. This subcommittee was charged with monitoring and coordinating the



implementation of Mexico's NCS (Estrategia Nacional de Ciberseguridad, or ENCS) in collaboration with the different dependencies and entities of the Public Administration. The subcommittee was also made responsible for promoting inter-institutional collaboration and cooperation schemes on cybersecurity and fostering collaboration and cooperation with the different stakeholders, including civil society, private sector, technical, and academic communities. In the case of Objective V National Security, the Cybersecurity Subcommittee is linked to the National Security Council through the Specialized Committee on Information Security (CESI).

In Uruguay, each organization that participates in the Uruguay Digital Agenda (Agenda Uruguay Digital or AUD) works on the creation and approval of its strategic plan, which generally coincides with the AUD regarding its period. The AUD consolidates the main initiatives of all the actors that make up the council, seeking their alignment with the government's policies and priorities. AGESIC has two roles with respect to the AUD. On the one hand, through the council, it coordinates and promotes its design and approval and its monitoring during execution. On the other hand, it is responsible for some of the goals of the AUD, so it also participates in the council as executor.

ESTABLISHING A MULTISTAKEHOLDER IMPLEMENTATION COMMITTEE

As noted in Part Two, there are many reasons to make sure any committee that is involved in an NCS represents a broad set of relevant stakeholders. When developing the NCS, a multistakeholder collaboration supports an important diversity of understanding and expectations for cybersecurity and encourages buy-in when it comes time to implement the guidance offered by the NCS. This is equally important in the implementation phase.

An important aspect to consider, however, is that with multiple stakeholders will come competing priorities. It is important that the implementation team stay focused on the strategic guidance offered by the NCS. There are sometimes dependent activities identified during implementation planning. For example, there could be other processes (such as cybercrime legislation) that require their own dedicated efforts. Those items must be identified and tasked to the proper organization to deal with them, leaving the multistakeholder group assigned to implementing the NCS to focus on the immediate goals. In collaborating with the government or competent authority for the implementation of a cybersecurity strategy, stakeholders are investing in their interests (commercial, personal, data related, etc.). It is important that stakeholders involved in the implementation process understand their responsibilities and what is required of them.

PRIORITIZATION CONSIDERATIONS FOR IMPLEMENTATION

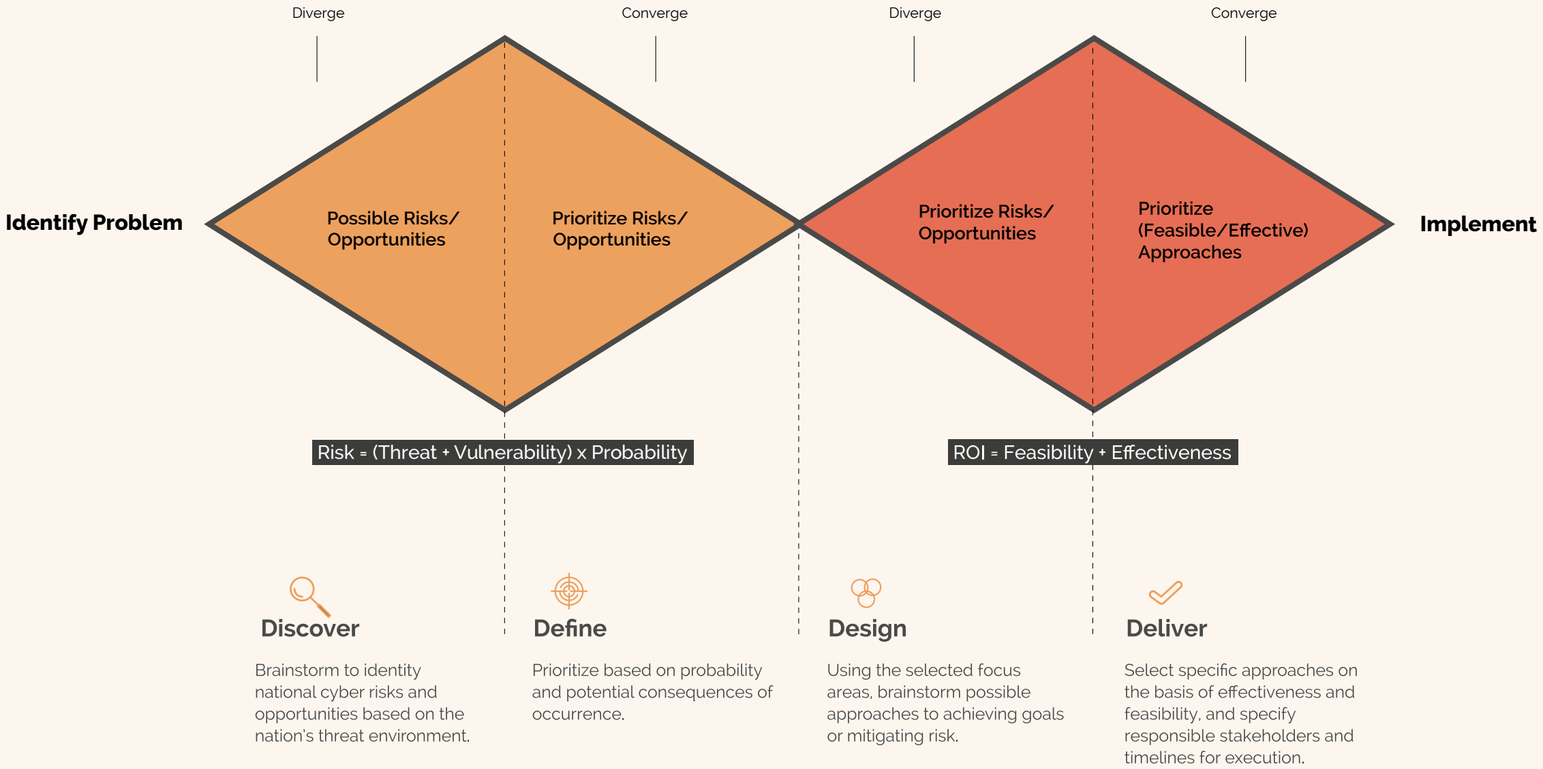
Many countries find the process of developing an NCS or a capacity-building plan diverts them into discussions of technology and standards (both important), which potentially result in a lack of focus on the 'why' of their initial decision to commit to cyber capacity building. As a result, countries may find they have a strategy or plan that has a dozen of goals and many dozens (in some cases, more than 100) implementation initiatives. This reflects, in part, the breadth of a nation's cyber capacity opportunity space. Because ICT and digital technologies and services affect nearly every aspect of national security, economic prosperity, and governance, it can be very difficult to narrow the potential list of strategy initiatives to a manageable number. Ironically, the better the country's strategic planning team did at involving all relevant stakeholders' perspectives and goals in the strategy, the harder narrowing the list may be because selecting some activities over others may risk eliminating the top interests of particular stakeholder groups. In general, a general best practice is to focus on no more than 15-25 initiatives, distributed across no more than five Goals or Objectives, over the life of a particular iteration of the strategic plan. But how can countries identify which of the many activities they've identified they should focus on?

One method for doing this is derived from international Design Thinking principles (see more in Annexes A and B), which focus on an iterative cycle of ideation, refinement, and prioritization and can be easily adapted to the strategy-to-implementation challenge. Design Thinking is a model intended to help multistakeholder groups come to a consensus on the most effective ways to envision and implement their products or goals. The full Design Thinking cycle is often depicted as a "double diamond" that can be adapted to cyber capacity building, as shown in Figure 4, representing recursive ideation and refinement steps:

The 'Double Diamond' process maps the divergent and convergent stages of a design process. Developed by the British Design Council and used in various forms by the Stanford d-School, the Harvard Business School, and other innovation leaders, it applies modes of thinking that designers use to solve real-world problems. The council's origin is Industrial Design, which is about creating tangible objects. As such, the model describes a linear process that ensures solutions are generally perfected before execution.

This method can also be applied to identifying and prioritizing Strategic Goals/Objectives, and for exploring and selecting Implementation initiatives.

Figure 4 **The Double Diamond of the Design Thinking Cycle**



In NCS development and implementation, the first two segments (Discover and Define) represent the implementation team's evaluation of their strategic risk/opportunity context, which they have distilled into goals and/or objectives. The next (Design) phase—identifying implementation initiatives—is also often captured in the strategic plan. The final convergence phase that narrows and prioritizes that list to what can actually be implemented with the available resources (Deliver) is frequently overlooked. This missed phase may be a result of several factors:

- The planning group doesn't want to eliminate or under-emphasize the interests of any one set of stakeholders;
- The strategy is a compromise document that reflects competing interests that could not be resolved in the strategy development phase;
- The government or team has no processes in place to prioritize resourcing requirements (all strategic initiatives are, at implementation, resourcing requirements);
- Political or environmental conditions have changed, and momentum was lost; or
- Simple "Planning Fatigue" – the strategy development phase itself exhausted the political will and negotiation space needed to undertake the difficult task of another down-selection round of decisions.

Whatever the reason, it is common for a strategic plan to include more initiatives than can be executed within existing resources. Thus, if the plan is to be implemented, the implementation team

must make decisions about which initiatives to fund or otherwise invest scarce human resources in pursuing. Prioritization is inherently difficult—factors weigh against one another, and proposals are variously attractive or prohibitive when viewed through different lenses. In addition, resources—people, money, time, political capital—spent on one priority are not available for others. Nevertheless, there are some approaches that can be helpful in the difficult task of prioritizing among initiatives. As with the development of the strategy itself, the more actively all stakeholders are involved in the prioritization, the better the outcome, and the broader the "buy-in" to the final implementation roadmap.

There are three key factors to consider in prioritizing implementation efforts: timelines, sequencing, and return on investment (ROI).

Timelines

Timelines are a prioritization consideration because different initiatives require different amounts of time to bear fruit. There is an adage that says, "the best time to plant an oak tree was 20 years ago…but the second-best time is now!" Some strategic initiatives are like oak trees—they will take years or even decades to mature, so if it is possible to start them immediately, it's a good idea to do so. The most common example of such an initiative is digital workforce development. Nearly every country faces a shortage of trained digital and/or cybersecurity professionals, and for some, it is a critical constraint on their ability to execute other capacity development or strategic goals. But it takes many years to develop a digitally savvy workforce with skills oriented to a knowledge economy. Nevertheless, with high attrition rates within governments for cybersecurity jobs and low rates of availability of cyber-specific educational opportunities, countries should give special consideration to prioritizing workforce-related initiatives so they can plan for and allocate the budget and expertise to get those programs established as early as possible.

Sequencing

Sequencing, in the context of prioritization, refers to which implementation initiatives depend on the completion of other initiatives or pre-requisite activities in order to be implemented. As a first step, the stakeholder team should examine the overall list and identify any activities that are necessarily pre-requisite to accomplishing others and group them accordingly. For example, if a strategy has several activities associated with protecting critical infrastructures and services, those that involve establishing criteria and processes for identifying those critical services and for establishing legal authorities to regulate their cybersecurity will need to be accomplished before any efforts to identify and implement international cybersecurity standards in the sectors or systems identified. "Annex A: Design Thinking and the "Roots & Fruits" exercise" later in this document offers an approach to sequencing.

Return on Investment

Although ROI is perhaps the most crucial factor in prioritization, it is often the hardest to determine. While ROI may sound dry and business-focused, it is the key link back to the 'why' of the strategic plan because it addresses the fundamental risks and opportunities the country faces by evaluating each activity according to the impact it can have on mitigating those risks and/or realizing those opportunities. There are different ways to consider ROI, most of which focus on cost and profit or savings, which can be difficult to assess for the kinds of complex activities addressed in most cyber strategies. For example, it is notoriously difficult to explain the ROI for cybersecurity technologies because they can be costly to purchase and sustain. The "return" is the avoidance or minimization of consequences of destructive incidents. ROI measured in cost or consequence avoidance is difficult to assess, even in terms of money, because it is hard to estimate the cost of an event that didn't happen. In addition to monetary costs, there are also potential "costs" related to loss of services, business, privacy, intellectual property, or even lives and safety. Therefore, rather than focus on cost and savings/profit, the approach described below uses effectiveness and feasibility as its measures. It is another Design Thinking tool specifically designed to assist in the final "convergence" phase.

THE PRIORITIZATION PROCESS

Annex B offers detailed information on how to organize a multistakeholder prioritization process using a proven Design Thinking method, but there are many possible approaches. Regardless of the path taken to get to a prioritized list, it is important to remind the stakeholders that not everything on the list will get done; the purpose of prioritization is to make hard decisions about what to do with available (and limited) resources.

It is also important to remember that cyber strategies are, ideally, iterative. This means that while a country may have a very large number of important objectives to achieve, they do not all have to be accomplished within one strategy cycle. Countries may find it useful to plot out a very high-level arc stretching ten years or more that describes their desired end-state in broad terms such as envisioned industrial or economic capacity, societal goals in education or employment, participation in regional or international activities, and so on. They can then arrange their desired initiatives along that arc, using the considerations discussed above to identify those activities that should be started immediately because they are time-consuming, pre-requisite to other initiatives, or particularly impactful, and then make an informed decision to readdress the remaining initiatives subsequent strategy cycles. Some organizations find Strategic Illustration, or capturing the "big picture" in an intuitive visual depiction, to be helpful in sustaining focus over a long period, even if short-term conditions change. Whatever method is chosen, capturing the long view can help reassure stakeholders that their priorities are not being neglected even if they are not addressed in the immediate implementation cycle, which may be focused on laying the strongest possible foundation for subsequent capacity growth.

The outputs of the prioritization process can facilitate the implementation plan in three ways:

1. Remind stakeholders of the importance of the national goals that must be achieved within a limited resource pool;
2. Significantly reduce the number of initiatives under consideration for this strategy cycle (in future cycles, changing conditions may change how particular initiatives are evaluated); and
3. Create consensus around the identified priorities.

Having all stakeholders participate in each step of the prioritization process helps ensure that most participants will accept the group's decision. Moreover, it provides them the opportunity to hear from the subject matter experts about why each initiative under consideration was ranked as it was. If the process is transparent and "follows the rules," participants will understand why the decisions were made and can convey that rationale to their constituents.

The ultimate purpose of prioritization is, of course, to facilitate implementation. Using the ROI exercise in Annex B (or another approach with a comparable outcome) and applying timeline considerations and dependencies (sequencing exercise in Annex A) allows planners to easily identify those items in the strategy that are most important to focus on in the current implementation cycle because they have long lead-times, are essential to future initiatives, have a high impact on strategic outcomes, or represent "quick wins." Related priorities may be combined into one more impactful program, potentially keeping more good ideas in the mix. Lower priority initiatives can be eliminated, if deemed to have little strategic impact, or shelved for later consideration. Remember: the goal should be a total of not more than 25 or so initiatives for any one implementation cycle.

Before declaring victory, there are a couple more activities that must occur before the group will have a complete implementation plan: stakeholder mapping and resource tagging. Stakeholder mapping simply involves assigning each of the prioritized initiatives to a responsible office and specifying what support they should receive from other offices. Resource tagging in this case means notionally identifying where the resources will come from to implement this initiative. This often involves some mix of national and beneficiary resourcing (the beneficiary is the entity most affected by the initiative, usually in cyber-related initiatives the system or function owner), where the relative contributions are determined at least in part by the degree to which the initiative benefits more than one stakeholder (the more stakeholders or beneficiaries, the more

national resourcing is typically allocated).

A couple of notes about resourcing:

- Ideally, this should be done within the broader context of, and in the same process as "normal" national budgeting, The strategic initiatives supporting the cyber implementation plan should be weighed alongside other national investments such as building infrastructure, expanding connectivity, securing borders, etc.
- Look for synergistic opportunities. Major priorities like infrastructure and national security nearly always have cyber components. Funding them together with related cyber implementation plan items can reduce overall costs, ensure mission alignment throughout execution, and increase the likelihood of completion. For example, road-building involves a substantial expenditure for excavation, which provides an opportunity to lay the cable that can support future broadband connectivity to the same regions at a much lower cost. Similarly, infrastructure modernization can offer the opportunity to build in cybersecurity protections much more cost-effectively than applying them in a separate "cyber" program after the fact.
- Look for ways to offset impact to national budgets. Ideally, this is done during the ideation phase, but it is worth another look during resourcing. Are there potential partners who could share the cost? Are there external funding sources, such as donor nations or NGOs, whose interests align with particular initiatives?
- Resource planning is always somewhat notional. In every cycle, unanticipated needs will arise that must be met, and planned expenditures will not be executable, freeing up funds. Nevertheless, the process should be treated seriously, with a conservative view that assumes more unexpected costs than windfalls. There is always somewhere to use extra money and people (such as Quick Win initiatives!) but falling short on funding part-way through execution can result in delays and changing circumstances that drastically increase cost or complexity, or even make the project inexecutable (for instance, if political priorities change). For this reason, it is better to select fewer initiatives than you expect to be able to support, since you can always add the next item below the cut line, but you cannot always salvage an underfunded effort.
- Sustainment is absolutely essential in cyber programs. Purchasing a new capability but allowing the licensing to lapse after the trial period can introduce more vulnerabilities than not having that tool at all, or in the case of e-services, can undermine public trust. Licensing is expensive, so it is important to account for the outyear costs when developing budgets in order to accurately plan for the sustainment of previously implemented or in-progress initiatives.
- Suppliers of major systems will often offer substantial discounts to governments or strategic partners. It is worth asking, but read the fine print (that is, make sure there is nothing in such an agreement that works against national interests). Cybersecurity is national security; it is worth paying more for a trustworthy product.
- People are resources. All the money in the world will not enable a project if there are not enough trained professionals to implement and sustain it. Human resources are a significant part of implementation costs and should be included in estimates. Since nearly every cyber capacity-building initiative will require trained personnel, it is a good idea to try to achieve economies of scale by identifying common skills requirements across initiatives (and existing programs) and investing in workforce development programs.

This brings us back to ROI. In the prioritization exercise, participants will have identified initiatives that were identified as "strategic investments." By definition, these efforts are difficult and/or costly, so they will take a disproportionate toll on available resources. But because they can have a significant long-term impact, they should be considered as top priorities anyway. It is likely that only a very few—perhaps only one or two—of these can be implemented within anticipated resources. In that case, it is a good idea to go back to the timeframe and sequencing considerations discussed early in this chapter. The longer an investment is going to take to mature, and/or the more objectives and initiatives to which it contributes, the more seriously it should be considered for implementation during the current cycle. In addition, strategic investments are often the kinds of efforts that outside funding sources, such as donor nations, the World Bank, or others may be willing to assist with. Of course, it is important that national decision-makers understand the full ramifications of such offers, including

trade-offs between grants versus loans, expected reciprocal actions, usage or implementation expectations or constraints, or other restrictions or requirements that may hinder national aspirations in the future when they go into effect.

MONITORING AND EVALUATION

Evaluation planning needs to ensure that outputs are linked to the outcomes and long-term impact of the program. NCS objectives are often general and broad. As a result, being able to identify concrete indicators for the measurement of success can be difficult. Evaluation allows a thorough examination at each layer on the effectiveness of the NCS's long-term impact. Thinking about it in layers, the evaluation will need to drill down to determine the effectiveness of the overarching ethos of the NCS and how it was driven down through and to the various stakeholders.

Another aspect rarely considered is the questions of how this evaluation will be undertaken and who will manage the process. Will or should it be the government or an external evaluator, an independent group, or the original group of stakeholders who probably had an appreciation of the original intent of the NCS?

Creating a monitoring and evaluation (M&E) framework to monitor implementation activities means building in the metrics early in the process. Having the metrics embedded early on helps keep nations on track during their development stage and keeps each stakeholder accountable for their piece of the puzzle. The M&E framework allows a nation to monitor implementation activities while measuring effectiveness. This approach can only be successful if Key Performance Indicators (KPIs) were set before as part of the planning process. There is a plethoric number of resources on the formulation and measurement of cybersecurity-related KPIs at the organizational level. Some will still argue, however, that there are no universally recognized, generally accepted metrics by which to measure and describe cybersecurity improvements. As a result, decision-makers are left to make choices about cybersecurity implementation based on qualitative measures rather than quantitative ones.

Cyber resiliency metrics, one of the criteria to consider measuring, are powerful indicators in their own right. According to MITRE's Cyber Resiliency Engineering Framework (CREF), cyber resiliency metrics can inform investment and design decisions. They are closely related to, but not identical with, metrics for system resilience and security and share challenges related to definition and evaluation with such metrics. A cyber resiliency metric is derived from, or relatable to, some element of the CREF such as a cyber resiliency goal, objective, design principle, technique, or implementation approach to a technique.

At the national level, measuring and evaluating the effectiveness of an NCS can be a daunting task. In several OAS Cybersecurity Reports, governments across the LAC region have identified that the lack of human capacity to detect cybersecurity threats—let alone to monitor these threats—is a major challenge. Understanding the tools available for M&E is an important part of being able to implement the NCS. Being able to identify funding to procure, train, and retain the human capital needed to use those tools is also a critical factor that will influence M&E and so the effectiveness of the NCS.

At the organizational level, measuring the success of implementation can be linked to compliance with an established organizational standard (e.g., the ISO 27000 series). The effectiveness of this measure is based on the performance of the organization to implement its pre-planned response plan to a real-time cyber threat.

While the state will work to establish the broad environment of cybersecurity resilience or preparedness that they aspire for, at the organizational level, public and private sector organizations should be guided by baseline security requirements issued for them. According to ENISA, *"defining a minimum set of security measures is a complex exercise that should take into account the following aspects: the different level of maturity among the stakeholders, the differences in terms of the operational capacity of each organization and the different standards existing in each critical sector under consideration."*

ENISA also advises that implementers ensure that the scope of the evaluation, key objectives, and expected outcome with its timeline are defined at the onset. Additional critical actions include:

1. Identifying the roles and responsibilities of key stakeholders, requiring that they follow both a quantitative and qualitative approach, giving emphasis on both impact and result;
2. Performing an external impact assessment for each activity of the strategy taking into consideration the opinion of external and/or affected users/communities;
3. Evaluating each activity against the action plan and key performance indicators (KPIs) agreed upon when the activity kicked off;
4. Identifying lessons, good practices, and bad practices from the internal and external impact assessment as well as the evaluation of each activity; and
5. Preparing an analytical evaluation report describing the achieved results and the expectations for the next evaluation.

As discussed earlier under the CRI model, understanding cybersecurity from an economic benefit perspective can shape the level of priority given to cybersecurity efforts at a national level. While not endorsing one assessment tool over the other, we believe it is important to highlight that there is a tangible cost-benefit of the impact that investments in cybersecurity can have.

According to FIREEYE, at the organizational level,

> "[c]yber risk must be considered a living scale… If we understand the key business processes, we can understand how technology enables this and therefore assign an impact level if that asset were to be compromised. We can then start to qualify the relevant threats and probabilities of an incident to these assets. To quantify the impact we must then qualify the direct and indirect losses that would occur during an incident. Map these together and we now have the foundations of business risk profile that can be discussed and agreed with the business. This enables the most rudimentary measure of success."[95]

Through these lenses, one must consider the questions: What are the risks? Are the investments being made proportionate to the risks to guarantee success? Are policies, procedures, and people in place to ensure effective implementation?

EVOLVING CYBERSECURITY INFRASTRUCTURE

Society is changing quicker than we can imagine due to exponential technological advances, and many member states haven't decided how to regulate this as yet. Instances of new phenomena change quicker than our policies and legislation can maintain. Thinking ahead on future threats such as deepfakes may seem inconsistent with the current reality, but out-of-date structures will leave one vulnerable to the newest behavior enabled by technology. It is critical to think about planning for the future from a risk perspective. Understanding the threats and their impact (including mitigation measures) will aid in determining what any preceding strategy should be addressing. Therefore, the evaluation of an NCS can lead and guide institutional changes for the implementation of cybercrime legislation.

Uruguay's approach to M&E

AGESIC's Information Society coordinates the monitoring of the council's agenda and meetings. All the information resulting from the monitoring is uploaded to the Uruguay Digital portal, in a tool called "Mirador" whose objective is to inform the public about the AUD and the progress in each of its goals.

AGESIC developed a portfolio management and monitoring system aligned with the good practices promoted by the Project Management Institute. This system, called SIGES, is used internally by all the agency's projects as the main management tool for each project. At the same time, it also serves as a management knowledge center of portfolios and projects and the main source of information that automatically feeds a Balanced Scorecard (BSC, known in Spanish as a Cuadro de Mando Integral, or CMI). This CMI is reviewed and presented by the Strategic Management area to the direction of the agency and used by each of the agency's areas in the monitoring and follow-up of their projects.[97]

AGESIC offers SIGES the software to public government entities, and multiple public bodies use it to manage their portfolio. The implementation of the strategy is carried out through the execution of the agency's portfolio of programs and projects and evaluated based on the CMI in general terms and SIGES in detail. All Information Security projects are managed and evaluated in SIGES.

Notes

86 National Cybersecurity Framework Manual, https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

87 An evaluation framework for Cyber Security Strategies, 23, https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.

88 Created by the MITRE corporation and used with permission.

89 See the NCSS: An Implementation Guide for additional guidance on how to manage an NCS lifecycle: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

90 See for example: Matt Shealy, "Top cybersecurity KPIs to track for risk mitigation," Klipfolio, September 1, 2020, https://www.klipfolio.com/blog/top-cyber-security-kpis; Abi Tyas Tunggal, "14 Cybersecurity Metrics + KPIs You Must Track in 2021," UpGuard, September 14, 2021, https://www.upguard.com/blog/cybersecurity-metrics; Phoebe Fasuolo, "Top 20 Cybersecurity KPIs to Track in 2021," SecurityScorecard, July 8, 2019, https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track; and "10 Cybersecurity Metrics You Should Be Monitoring," Cipher, accessed September 19, 2021, https://cipher.com/blog/10-cybersecurity-metrics-you-should-be-monitoring/.

91 Robert S. Taylor, "How to Measure Cybersecurity," Lawfare, August 26, 2019, https://www.lawfareblog.com/how-measure-cybersecurity.

92 Deborah J. Bodeau, Richard D. Graubart, Rosalie M. McQuaid and John Woodill, Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring - Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods, (MITRE, 2018), https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.

93 See for example "ISO/IEC 27001 Information security management," International Organization for Standards, Technical Committee ISO/IEC JTC 1, Subcommittee SC 27, accessed April 22, 2022, https://www.iso.org/isoiec-27001-information-security.html.

94 ENISA, National Cybersecurity Strategies: Practical Guide on Development and Execution, 24, https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport.

95 Greg Day, "Measuring Success in Cybersecurity," FireEye, March 3, 2015, https://www.fireeye.com/blog/executive-perspective/2015/03/measuring_success.html.

96 Deepfakes have been defined as synthetic media in which a person in an existing image or video is replaced with someone else's likeness.

97 "Agenda Uruguay Digital 2025", Presidencia de la República, accessed April 22, 2022, https://uruguaydigital.gub.uy/.

Part **5**

CASE **STUDIES**

The Cybersecurity Program adherent to the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) has played a key role in supporting OAS member states' policy strategy formulation, implementation, and review. In the last decade, the Latin America and Caribbean (LAC) region has made continuous progress in formulating and implementing NCSs. Currently, a total of 17 OAS member states have approved their NCSs; 14 of these were able to do so with the technical support of CICTE/OAS. At the time of writing this publication, four countries are at various stages of initial strategy development or at the review stage, as well as one country (Colombia) has published more than one NCS. The focus of this section will be on the 14 member states that have received technical assistance from the OAS in the process of publishing their NCS.

COMMON NATIONAL CYBERSECURITY STRATEGY THEMES OF THE AMERICAS

Considering that the nature of the strategy is entrenched in a national digital perspective, every NCS is, and should be, customized to the reality and context of each country. Thereby, there are multiple approaches in which a strategy can be formulated and implemented. Even though there is no established consensus on what should constitute a strategy, common themes are observed globally.

This section covers NCSs in the following countries: Argentina, Belize, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, Guatemala, Jamaica, Mexico, Panama, Paraguay and Trinidad & Tobago. For the purpose of the comparative analysis, the strategies of each country are divided into subregions: Caribbean, Central America, and South America. For each subregion, a comparative analysis is provided based on the following three dimensions: drafting approach, objectives, and implementation. Furthermore, each section includes a summary table of the comparative variables analyzed according to common objectives addressed in the NCSs. The comparative tables are designed based on specific objectives related to each dimension. Further, to determine whether a particular country included such objectives within their respective NCSs, the inclusion of the minimal course of action for each country's strategy is taken into consideration or, in other words, the incorporation of action lines to achieve the intended policy goal.

Comparative Analysis of National Cybersecurity Strategies in the Caribbean

Table 1 **Comparative Table – Dimensions and Variables**

Approaches to Drafting	
V.1	**Information Assurance Issue**
V. 2	**National Security Issue**
V. 3	**Economic Issue**
V. 4	**Law Enforcement Issue**
Key Objectives and Lines of Action	
V.1	**Legal and Regulatory Frameworks**
V.1.1	Legislation
V.1.2	Defense and Cyber-Security
V.2	**Cybersecurity Culture**
V.2.1	Public Awareness Raising
V.3	**Multistakeholder Engagement**
V.3.1	Public Sector
V.3.2	Private Sector
V.3.3	International Relations
V.4	**Technical Capability/Capacity-building**
V.4.1	Incident Response
V.4.2	Critical Infrastructure Protection
V.4.3	Education, Research and Training
Policy Implementation	
V.1	**Policy Implementation Timeline**
V.2	**Governance Model**
V.3	**Operational Factors**

Approaches to Drafting

At the time of publication, three countries have developed an NCS in the Caribbean region: the Dominican Republic, Jamaica, and Trinidad and Tobago. Despite the clear difference in structure and format of each of the strategies, the content of all three address common themes and action lines –although with varying emphasis – such as the need to protect critical infrastructure, public awareness campaigns, the need to engage in multilateral collaboration with private and public entities, and the existence of a clear incentive to strengthen the nation's cybersecurity capabilities and standards.

Regarding the incentives for developing the NCS, the three nations identify a clear growing threat in cyberspace at the individual and collective levels. There is a clear recognition of the role of ICT in advancing national development while acknowledging the growing risks of an unprepared country to respond to the potential threats adjacent to the cyberspace environment. Although all approaches (information assurance issue, national security issue, economic issue, and law enforcement issue) are covered on Jamaica's NCS, the economic issue is perceived to be the dominant motive that shapes the course of action adopted on the strategy. This NCS of Jamaica highlights the particular cyberattack vulnerability of the financial sector due to its lucrative potential, the increasing presence of organized crime in cybercrimes, and the concerning physical threats to national critical infrastructure. Likewise, the overall approach to drafting the NCS of Trinidad and Tobago also centers on the economy. The strategy indicates high potential target entities of cybercrime, primarily focusing on the financial and industrial sectors. Thereby, the NCS of Trinidad and Tobago calls in particular to improve collaboration between the government and Internet Service Providers (ISPs), since these play a key role in the physical and digital implementation of the strategy.

The conglomerate of constitutional articles outlined in the Dominican Republic's NCS indicates that national security and development are the main approaches to drafting the regulation. The strategy, for instance, leverages Article 260 of the constitution, which states that combating international criminal activity that threatens the interest of civilians and the damages caused by technological disasters is considered a high national priority. In the Dominican Republic's NCS, ICT is seen as a vehicle towards improving public management, transparency, access to information, and digital development. The high dependency on ICT is critical for all areas of the Dominican Republic's society, including economic, social, and security development. This dependency calls for a need to implement measures that guarantee the protection of critical assets of state and private information. Overall, the NCSs of the Caribbean region emphasize the economy as the foundational element to draft their respective strategies.

Table 2 **Approaches to Drafting – Caribbean Region**

Approaches to Drafting a National Cybersecurity Strategy			
Variables	**Dominican Republic**	**Jamaica**	**Trinidad & Tobago**
Information Assurance Issue	X	X	X
National Security Issue	X	X	
Economic Issue	X	X	X
Law Enforcement Issue		X	

Key Objectives and Lines of Action

A commonality between all three countries of the Caribbean subregion is the creation of a Cybersecurity Incident Response Team (CSIRT) as a main priority. In the Dominican Republic and Jamaica, the CSIRTs will be established and operated in existing government bodies. In the Dominican Republic, the Dominican Institute of Telecommunications (INDOTEL) will be responsible for creating a national CSIRT, whereas in Jamaica, the Ministry of Science, Energy & Technology (responsible for ICT) will be the main operational body. In comparison, Trinidad and Tobago will create a new Trinidad and Tobago Cyber Security Agency (TTCSA) to operate the TT CSIRT.

The NCSs from Jamaica and Trinidad and Tobago explicitly call for cooperation between the established CSIRTs and the existing law enforcement bodies. In Trinidad and Tobago's case, the aim is to establish a focal point to manage cyber incidents. Jamaica goes further into stating that the purpose of establishing a line of communication between the two governmental entities is to cooperate on detecting cyber incidents, whether for an investigation or in the case that law enforcement detects a cyber incident. The NCS of the Dominican Republic outlines the creation of sectoral CSIRTs to improve intersectional coordination in the protection of information systems and critical infrastructure.

Table 3 **Technical Capability / Capacity-Building - Caribbean Region**

Technical Capability / Capacity-Building			
Incident Response	**Dominican Republic**	**Jamaica**	**Trinidad & Tobago**
Establishment of a National CSIRT	X	X	X
CSIRT Capacity at the National Level			
Identification and Management of Incidents		X	X
Information Sharing with Various Sectors	X	X	X
Reporting Mechanisms			
Establishment of Sectoral CSIRTs	X		

Policy implementation

The NCSs of the Dominican Republic and Jamaica coincide in the elaboration of an initial execution plan and a policy revision timeline. In the Dominican Republic case, within 90 days from the date the decree is published, an Action and Revision Plan must be established that outlines the priority activities, budgets, deadlines, and institutions responsible for implementation. The

plan will define an evaluation framework for monitoring and improvement purposes. In addition, within 60 days of this decree, relevant entities will present policies and action plans related to cybercrime, cyberterrorism, cyberdefense, cyberwar, and cryptography. After 18 months, if applicable, the strategy is stipulated to be revised and modified accordingly.

Likewise, the NCS of Jamaica calls for a revision period of the strategy every three years or as considered pertinent. The Jamaican NCS objectives and activities are categorized within a short-term (one year), medium-term (two years), and long-term (three years) priority basis. Within the short-term actions, Jamaica's NCS includes several key components, such as establishing the National CSIRT, developing research programs, and conducting a national survey on cybersecurity awareness. Similar to the Dominican Republic, within three months of adopting the Jamaican NCS, the Ministry responsible for ICT and the National Cyber Security Task Force (NCST) will be responsible for developing an implementation plan to enact the objectives, activities, and responsible entities outlined in the strategy.

Although Trinidad and Tobago's NCS does not outline an initial execution plan and revision timeline, it indicates that the strategy is based on the government's medium-term policy framework (2011-2014). The main priority is to establish the TTCSA as the main body responsible for all cybersecurity matters and a detailed organization structure for the TTCSA is provided. The scheme of the government entity portrays that besides an Executive and Deputy Director, multiple managers would be designated on areas, such as the cyber forensics/investigation unit, culture education/training, public and private partnerships, legal, TT CSIRT, among others.

Table 4 **Policy Implementation - Caribbean Region**

Technical Capability / Capacity-Building

Variables	Dominican Republic	Jamaica	Trinidad & Tobago
Policy Implementation Timeline			
Short Term (1-3 years)		X	
Medium Term (4-5 years)	X		X
Long Term (5-10 years)			
Governance Model			
Strategy Development Entity	X	X	
Coordinating Structure	X	X	X
Operational Response Entity	X	X	X
Multistakeholder Agency	X	X	
Operational Factors			
Monitoring and Evaluation	X	X	
Budget Allocation	X		
Priority Objectives	X	X	
Operational Plan	X	X	

Comparative Analysis of National Cybersecurity Strategies in Central America

Currently, five countries in Central America have approved NCSs with the support of the OAS: Belize, Costa Rica, Guatemala, Mexico, and Panama. All countries share the inclusion of provisions on critical infrastructure protection, explicitly outlined as part of their respective objectives. Panama takes this a step further, naming its NCS as the "National Cybersecurity Strategy and Protection of Infrastructure," in which objectives are formulated on the basis of critical infrastructure. Guatemala is the exception; while it does not explicitly include critical infrastructure protection as a key objective, it does include it as one of its three priority areas on information technology.

Approaches to Drafting

Economic and information assurance issues are the predominant elements that guide the NCSs development in Central America. With the exception of Mexico, all countries involve information assurance as a key issue that persuades the NCS approach. The NCS of Mexico differs in that it establishes the economic issue as the central component that drives policy priority actions on cybersecurity matters. The main objective of Mexico's strategy is the establishment and strengthening of cybersecurity actions to enable the population, as well as private and public organizations, to use ICTs responsibly for the sustainable development of the state.

Likewise, Costa Rica incorporates the economic aspect as a primary focus on elaborating the NCS, as well as a transversal theme of respecting fundamental human rights, intending to develop an orientation framework for the country's actions on the safe use of ICT and fostering stakeholder coordination and cooperation. Similarly, during the Costa Rican sectoral NCS development consultations, multistakeholder feedback indicated the need for national coordination on cybersecurity efforts as a central factor to include in the NCS. The promotion of the safe use of ICT is considered an instrument for enhancing the quality of life, in which the implementation of Costa Rica's strategy will direct the country towards continuing to be a regional leader in the investigation, development, and human resource of ICT.

Panama also considers it to be "vital for the population and economic wellbeing" that the strategy is oriented towards national cybersecurity enhancement, emphasizing critical infrastructure. The NCS of Panama has multiple approaches to drafting, including economic, national security, and law enforcement, aiming to increase national cybersecurity that allows the reliable use of information technologies and an economic and regulatory environment favorable to companies' development and functioning of the state.

Along with Panama, the NCS of Belize identifies its purpose in protecting the Belizean people and economy. The strategic vision aspires to capitalize on the opportunities of the digital economy to improve the standards of living of Belizean society. Even though the primary approach to drafting is an economic issue, the Belize NCS includes information assurance and national security issues as essential national elements.

Information assurance and national security issues shape Guatemala's NCS, which proposes strengthening the nation's cybersecurity capabilities to ensure the participation, development, and exercise of people's rights in cyberspace.

Table 5 **Approaches to Drafting - Central America Region**

Approaches to Drafting a National Cybersecurity Strategy

Variables	Belize	Costa Rica	Guatemala	Mexico	Panama
Information Assurance Issue	X	X	X		X
National Security Issue			X		
Economic Issue	X	X		X	X
Law Enforcement Issue	X				X

Key Objectives and Lines of Action

Whether for drafting or revising existing law, the need for cybercrime legislation is a commonality in the Central America region. Framed within their NCSs, Belize and Guatemala include an international component to draft cybercrime legislation. In the case of Belize, the legislation stipulates the creation of a legal working group that consults for legal assistance with international organizations, including the OAS, on the development of a cybercrime bill. The NCS of Guatemala, similarly, indicates that the law against cybercrime must refer to international standards that are applicable to the country's reality. In contrast, efforts on cybercrime legislation for Costa Rica, Mexico, and Panama centered on the need for the revision of existing legislation to be aligned with cybercrime considerations. Costa Rica plans to revise current legislation to guarantee adequate cybercrime procedural tools by creating a specialized commission. For the NCSs of Mexico and Panama, the purpose of revising existing legislation is to analyze and propose legislative modifications, harmonization, and development of judicial capabilities to provide cybersecurity legislation alignment.

Table 6 **Legal and Regulatory Frameworks - Central America Region**

Legal and Regulatory Frameworks

Variables	Belize	Costa Rica	Guatemala	Mexico	Panama
Legislative Frameworks for ICT Security					
Human Rights Online					
Data Protection Legislation				X	X
Intellectual Property Legislation					
Cybercrime Legislation	X		X		
Publication of Technical Standards			X		
Review Existing Laws	X	X		X	
Critical Infrastructure Law		X	X	X	

Policy Implementation

Within the policy strategy framework, the inclusion of an implementation timeline is only a consideration in the NCSs of Belize and Mexico. Considering the latter, the strategy outlines that the vision is that by 2030 Mexico will be a resilient nation in the face of cyberspace threats, capitalizing on the potential of ICT for sustainable development. Compared to Mexico's long-term timeline, Belize contemplates a three-year window (2020-2023) to implement the strategy. The Belizean NCS objectives, activities, and coordinating institutions are categorized within short-term

(six months), medium-term (one year), and long-term (two years) priorities to facilitate policy implementation. In this regard, there are four short-term objectives in the strategy: participation in international cybersecurity agreements, standards for information systems used in critical infrastructure, cybersecurity awareness initiatives, and a cybersecurity component to existing youth forums. Moreover, the NCS of Belize includes a timeline for monitoring and evaluation, as it stipulates that the achievements of the strategy will be reviewed after eighteen months of approval.

In the Central America region, the strategies differ regarding the ministry proceeding with the policy implementation. Costa Rica, for instance, intends that the Minister of Science, Technology and Telecommunication will delegate a national coordinator and a Consultive Committee, which will jointly be responsible for the strategy implementation and coordination. Belize also includes a national coordinator and a consultant body, in this case, the Inter-institutional Cybersecurity Task Force, both entities under the Ministry of National Security. Within the National System of Security framework, the NCS of Guatemala outlines that two committees will be created, the National Cybersecurity Committee and the Cybersecurity Technical Committee. The policy strategy of Mexico considers the establishment of a Cybersecurity Subcommittee, chaired by the Ministry of the Interior through the Federal Police/Scientific division. Differentiating from the previous NCSs, Panama is the only country that does not include a coordinating entity framework for the strategy implementation.

Table 7 **Policy Implementation - Central America Region**

Policy Implementation

Variables	Belize	Costa Rica	Guatemala	Mexico	Panama
Policy Implementation Timeline					
Short Term (1-3 years)					
Medium Term (4-5 years)	X				
Long Term (5-10 years)				X	
Governance Model					
Strategy Development Entity	X	X	X	X	X
Coordinating Structure	X	X	X	X	
Operational Response Entity		X	X		X
Multistakeholder Agency	X	X	X	X	
Operational Factors					
Monitoring and Evaluation	X	X	X	X	
Budget Allocation			X		
Priority Objectives	X				
Operational Plan		X	X		

Comparative Analysis of National Cybersecurity Strategies in South America

In the South America region, the OAS has supported six countries in elaborating their approved NCSs: Argentina, Brazil, Chile, Colombia, Ecuador and Paraguay. Although designed along different lines of action and objectives, there are four common areas addressed by all the NCSs: economic concerns; revising and updating existing cybercrime-related legislation; developing sector-specific campaigns to enhance cybersecurity culture at the national level; and developing academic programs to enhance cybersecurity culture at the national level.

Approaches to Drafting

The South American region is associated with a high number of cyberattacks. With the exception of Paraguay, the NCSs of the region regard national security as a motivator to drafting their respective cybersecurity strategies. Along with national security, the Ecuadorian NCS focuses on information assurance and seeks to guarantee the rights and liberties of citizens by building and strengthening national cybersecurity capacities, as well as ensuring the protection of the state's legal assets in cyberspace, ultimately contributing to national economic and human development.

The Chilean NCS highlights that the country, along with Argentina, Brazil, and Colombia, registers the highest number of cyberattacks in Latin America, particularly involving the access or theft of information. The cybersecurity policy highlights the potential impact of transnational cybercrimes perpetrated in Chile on the country's critical infrastructure, such as espionage and fraud. The conviction of Chile's foreign policy on multilateral diplomacy, focusing on international transparency and trust-building, aspires to decrease the risks of cyberspace conflict. Similar to Chile, the use of cyberspace for military purposes is articulated in the Argentinian NCS. The strategy of Argentina calls for the promotion of cooperation and dialogue in international forums to mitigate possible arm conflicts utilizing cyberspace. Chile's strategy notes that at the national level, cybercrime law and the protection of private life law ought to be reviewed and amended by the guidelines defined in the NCS. Within this context, the Brazilian National Cybersecurity Strategy – E-Ciber identifies that the lack of cybercrime legislation induces Brazil to be one of the leading global hosts of phishing sites. In this regard, the Brazilian NCS regards phishing, cyber espionage, and private information leaks as national threats.

Colombia's multiple published NCSs demonstrate the country's cybersecurity policy engagement. Fostering digital confidence and cybersecurity are the primary concerns addressed in the Colombian strategy. This is a result of the understanding that digital deficiencies increase cyberattack vulnerability, which often culminates in a decrease in confidence and a negative impact on socioeconomic development. The 2020 Colombian cybersecurity policy recognizes that the digital confidence gap of previous NCSs centers on the limited multistakeholder involvement. Furthermore, the strategy emphasizes that children, as they increasingly navigate online, are particularly exposed to the dangers and threats of cyberspace given the high cybercrime and low levels of child cybersecurity protection in Colombia. Likewise, the NCS of Paraguay highlights cyberthreats that impact children and youth, including child pornography, cyberbullying, grooming, and sexting. The Paraguayan National Plan of Cybersecurity is mainly based on an economic approach, aiming to foster the reliable use of ICT and an economic environment favorable to the development, innovation, and competitiveness of new technologies. Overall, by increasing cybersecurity, the South America region seeks to improve its fight against cybercrime, ultimately enabling digital development in the region.

Table 8 **Approaches to Drafting - South America Region**

Approaches to Drafting a National Cybersecurity Strategy

Variables	Argentina	Brazil	Chile	Colombia	Ecuador	Paraguay
Information Assurance Issue	X	X	X	X		
National Security Issue	X	X	X	X	X	
Economic Issue	X	X	X	X	X	X
Law Enforcement Issue						X

Key Objectives and Lines of Action

While the promotion of the cybersecurity industry is included in all NCSs of the South American region to various extents, the courses of action, purpose, and implementation differs. The NCSs of Argentina, Brazil, Chile, and Paraguay highlight Research, Development, and Innovation (RD&I) initiatives as essential to generating cybersecurity solutions and promoting the development of the industry at the national level. In the case of Argentina, the NCS seeks to foster RD&I to protect national systems in the face of cyberthreats. Brazil and Paraguay coincide in the alignment of joint efforts to conduct RD&I. Concerning the latter, the National Cybersecurity Plan of Paraguay stipulates the joint effort of academia, NGOs, research centers, and the public and private sectors to amplify cybersecurity and research projects. In the case of Brazil, the strategy seeks to align academic projects with production needs to encourage cybersecurity solutions. The E-Ciber of Brazil identifies the need for RD&I to cultivate innovation for national production, highlighting the prioritization of research on cryptography applicability. Similarly, the Chilean cybersecurity policy aims to create programs that foster national cybersecurity products and services export, supported by studies that analyze the global cybersecurity supply and demand.

Brazil, Colombia, and Paraguay consider education as a vehicle towards developing their cybersecurity industry, as education fosters the advancement of the required human labor force. Brazil and Paraguay propose including cybersecurity knowledge at all education levels, from early childhood to higher education. The Brazilian NCS highlights that the lack of human resources is the most significant deficiency to combat cybercrimes, as the talent gap directly impacts organizations' vulnerability to cyberthreats. The strategy recommends including technical courses, specifically software development in high school and higher education curriculum. Paraguay's NCS regards the inclusion of cybersecurity knowledge in primary education as an initial step to foster the interest of future professionals in the field. Similarly, to strengthen industrial development in cybersecurity goods and services, the Colombian NCS mentions that the Ministry of Information Technology and Communications will elaborate and implement a strategy to promote a national qualified labor force in the cybersecurity sector. Ecuador considers that legislative proposals should be developed to update and enhance existing legal frameworks on information security incident management.

Table 9 **Multistakeholder Engagement - South America Region**

Multistakeholder Engagement

Variables	Argentina	Brazil	Chile	Colombia	Ecuador	Paraguay
Standards/Guidelines		X	X	X		X
Information Sharing			X			

Multistakeholder Engagement

Variables	Argentina	Brazil	Chile	Colombia	Ecuador	Paraguay
Coordination and Cooperation	X				X	X
Capacity Building	X		X	X	X	
Domestic Industry Development	X	X	X	X		X
e-Governance						

Policy Implementation

Four NCSs from the region, Brazil, Chile, Colombia and Ecuador, include policy implementation timelines. The Brazilian NCS validity timeline is within a medium-term (2020-2021) period. In comparison, with an approximate allocated public investment of 8.42 million pesos, the strategy of Colombia is to be implemented within a short-term (2020-2022) timeline. The budgetary and physical execution of the objectives will be revised every six months within the time frame of the NCS. Further, the resource allocation for each responsible implementing entity is subject to their adequate objective compliance and spending according to the proposed yearly budget. In comparison, the cybersecurity policy of Chile is composed of two elements: a state policy with long-term objectives expected to be implemented within a medium-term (2017-2022) timeline and an agenda with short-term (2017-2018) measures. The short-term measures are set to be implemented by the current administration, leaving the following administration with the responsibility to revise the NCS and propose a new cybersecurity policy agenda that the next administration can execute. The objective of the Chilean contemplated policy implementation timelines is to ensure policy continuity and prioritization of the long-term objectives ascribed to the NCS. The public and private sectors will jointly be responsible for revising the Chilean NCS by the end of the first implementation year (2017). Ecuador contemplates a three-year window (2020-2023) to implement the strategy and suggests revising the policy instrument every two years or on the occasion that an institutional mandate changes, in order to verify the effectiveness and efficiency of the lines of action proposed. The Paraguayan NCS will be reviewed every three years or as considered pertinent. Additionally, the Paraguayan government will make periodic cybersecurity policy accountability reports available to the public to ensure transparency.

Within the implementation structure, the strategies differ on the public entity that will proceed with the NCS implementation and the number of stakeholders involved in the governance framework. The Chilean NCS, for instance, indicates that a cybersecurity bill will be prepared to consolidate the institutional framework responsible for the policy implementation. While the cybersecurity bill is approved, the Inter-Ministerial Cybersecurity Committee will be the coordinating and monitoring entity of the Chilean NCS. The CSIRT Gov will be responsible for technical incident management. Additionally, an inter-agency working group will be established to address international cyberspace issues, and the creation of an advisory consulting council conformed of different sectors will be evaluated. Likewise, the Brazilian NCS will establish a national cybersecurity council composed of state and non-state actors. The governance model of Brazil is composed of three entities responsible for policy implementation. The coordination will be proceeded by the Institutional Security Office of the Presidency of the Republic, the Ministry of Defense will be responsible for cyber defense actions, and the CSIRT Gov will be granted national competencies for incident response coordination.

In the case of Paraguay, the strategy notes that a delegated National Cybersecurity Coordinator will administrate the National Cybersecurity Commission, responsible for coordination and monitoring implementation. Moreover, specialized committees responsible for implementation will be established for each of the seven objectives outlined in Paraguay's NCS. In contrast, Colombia does not contemplate a centralized coordinating entity, and rather eight different

public entities will be responsible for implementing their corresponding lines of actions outlined in the NCS. Although Argentina excludes a governance implementation framework, the strategy mentions that the National Executive Power formulated the NCS.

In the case of Ecuador, the NCS proposes that the President of the Republic's Office and Sectoral Security Cabinet establish an institutional framework to create a collegial body, the Cybersecurity Committee.

Table 10 **Policy Implementation - South America Region**

Multistakeholder Engagement

Variables	Argentina	Brazil	Chile	Colombia	Ecuador	Paraguay
Policy Implementation Timeline						
Short Term (1-3 years)			X	X		
Medium Term (4-5 years)		X	X		X	
Long Term (5-10 years)						
Governance Model						
Strategy Development Entity		X	X		X	X
Coordinating Structure		X	X	X	X	X
Operational Response Entity		X	X		X	
Operational Factors						
Monitoring and Evaluation			X	X		
Budget Allocation				X		
Relationships with Stakeholders						
Key Objectives				X		

REGIONAL APPLICATION OF AN ASSESSMENT TOOL

In cyberspace, no one is an island and no country is isolated from its neighbor, whether they are landlocked or separated geographically by water. Recognizing that fact, the Organization of American States and the Inter-American Development Bank (OAS-IDB) met at the end of 2014 to begin planning a holistic study on the cybersecurity capabilities of countries in the LAC region. Both worked together with the Global Cybersecurity Center at the University of Oxford to design an online tool to implement the CMM, which uses 23 factors covering dimensions of cybersecurity. By using this tool, OAS-IDB gathered data from cybersecurity stakeholders representing different sectors; this information was validated with the support of member states. These stakeholders included government agencies, critical infrastructure operators, the military, law enforcement, the private sector, and academia. The conclusions in the report, ultimately published in 2016, were reviewed by the OAS-IDB, the University of Oxford, and the Potomac Institute for Policy Studies, and included contributions of international experts on cybersecurity in the hemisphere.

The final report, *Cybersecurity: Are we ready in Latin America and the Caribbean*, was the culmination of the widest application of the CMM yet undertaken at that time, as it was applied to 32 countries within one year. While the report represented a snapshot in time of an ever-changing landscape, it continues to provide a better understanding of the strengths and challenges in cybersecurity in each country. The conclusions highlight a hard reality: the region must do a lot more work in cybersecurity to ensure the cyber borders are as secure as physical borders.

This report also shows that the LAC regions were accelerating their focus on cybersecurity and moving it to the top of their policy and social agenda. It was also evident in the report that the 32 participating countries had different approaches, attitudes, and priorities towards cybersecurity. That said, governments generally recognized the importance of providing affordable access to ICT services for business innovation, growth, and the delivery of public services. Even with that recognition, however, Internet penetration was quite low in roughly half of the LAC region. Economic development initiatives across the region are calling for broadband investments and infrastructure modernization to propel their countries into the digital age. Additionally, adopting an NCS is arguably

one of the most important elements of a country's commitment to securing the cyberinfrastructure, services, and ICT business environment upon which its digital future and economic wellbeing depend. Some LAC countries have prioritized cybersecurity as a national concern and are establishing formal cybersecurity policies and building the capacities of relevant agencies.

Since that first report, a second edition was released in 2020, *Cybersecurity: Risks, Progress and the Way Forward for Latin America and the Caribbean*. This edition is built on the first and provides the countries of LAC with a picture of the state of cybersecurity and guidance about the next steps that should be pursued to strengthen national cybersecurity capacities.

Meanwhile, cyberattacks in the region have been increasing, mainly targeting LAC financial institutions. The COVID-19 pandemic and the increase in digital activity generated in the region have further exposed the vulnerabilities of the digital space in LAC. Every year, millions of new LAC users connect to the Internet for the first time, creating a reservoir of new customers who are less knowledgeable about technology than more mature digital customers. This contributes to an environment of heightened risk. Therefore, not only is LAC a target to these types of attacks, but it is also a significant source of them.

The second edition has given the region a refreshed vision on where it is and the opportunities that can be capitalized. For instance, although LAC countries have enhanced their cybersecurity capacities since 2016, the average maturity level of the region is still between 1 and 2 according to the CMM, in which 1 stands for Start-up and 5 stands for Dynamic or Advanced. In other words, most countries in LAC have started formulating some cybersecurity initiatives, including capacity-building measures. More significantly, some of these are already in place; however, they are being implemented in an ad-hoc manner, lacking coordination among key stakeholders. Low scores aside, the average maturity level of the 32 countries' cybersecurity should not overshadow the strides taken by the region over the past years.

From the analysis, the cybersecurity maturity level of the Southern Cone subregion was the highest in all of the five CMM dimensions, with an average between 2 and 3. Although "Legal and Regulatory Frameworks" was the most developed dimension, "Standards, Organizations, and Technologies" had the most significant improvement since 2016. It is noteworthy that all dimensions present similar levels of cybersecurity maturity, which suggests that countries in this region are addressing cybersecurity from a comprehensive perspective.

On the other hand, the Andean Group had an average cybersecurity maturity level of 2, slightly lower than the Southern Cone. This disparity highlights the importance of focusing cybersecurity efforts to strengthen the deployment of cybersecurity standards and technical controls in the region and to encourage responsible disclosure. In the case of Central America and Mexico, they presented an average maturity level of 2 in the "Cyberculture and Society" and "Cybersecurity Education, Training and Skills" dimensions, while the "Cybersecurity Policy and Strategy" and "Standards, Organizations, and Technologies" dimensions are below 2. Like in the Andean Group, Central America and Mexico should focus on enhancing the deployment of cybersecurity standards and technical controls, as well as encourage the development of a cybersecurity marketplace. Notably, the "Legal and Regulatory Frameworks" dimension has a maturity level between 2 and 3.

Finally, the Caribbean region has a maturity level between 1 and 2 in all dimensions. However, while "Legal and Regulatory Frameworks" was the most mature dimension, as it was in 2016, "Cybersecurity Policy and Strategy" remains the least mature. Developing an NCS provides a country with a more strategic and comprehensive approach that addresses and allows a better understanding of cybersecurity challenges. Likewise, this strategic planning allows for the prioritization of their objectives and investments in cybersecurity.

MARITIME SECTOR

Reflection

The great challenges of cybersecurity, like those of the Internet itself, are global. Therefore, it is critical that the countries of LAC must continue to foster greater cooperation among themselves while involving all relevant actors, as well as establishing a mechanism for monitoring, analysis, and impact assessment related to cybersecurity both nationally and regionally. More data concerning cybersecurity would allow for the introduction of a culture of cyber risk management that needs to be extended in both the public and private sectors.

Countries must be prepared to adapt quickly to a dynamic environment and make decisions based on a constantly changing threat landscape. Member states may manage these risks by understanding the impact and likelihood of cyber threats to their citizens, organizations, and critical national infrastructure. Moving to the next level of maturity will require a comprehensive and sustainable cybersecurity policy, supported by the country's political agenda, with the allocation of financial resources and qualified human capital to carry it out.

Recognizing that NCSs provide broad guidance at the national level, it is critical to translate this guidance in a more practical day-to-day application for the various stakeholders, including at the sectoral level. While every sector will have its own particulars and nuances, there are key concepts, considerations, and questions that need to be addressed when approaching cybersecurity at the sectoral level.

Among recent cyber incidents was the SolarWinds attack. This attack saw hackers use backdoors to spy on high-level public and private US entities. Similarly damaging, the DarkSide ransomware attack on the Colonial Pipeline cut off 45% of the East Coast fuel supply. One of the most significant situations that has raised cyber concerns is that of the Ever Given. Stuck for six days across the Suez Canal, the ship blocked maritime trade through the Red Sea, leading to immediate global economic consequences. While officially an accident, many cyber experts remain concerned that it was an accident born of intentional cyber interference, likely with the operational technology on the ship. The role of the maritime domain in both the global economy and the critical supply chains on which humanity now relies makes it a prime target for attack – both by state and criminal actors. Focusing on applying cybersecurity frameworks to the maritime sector – one of the more overlooked domains of cyber concern – demonstrates some of the decisive points and potential pitfalls in the process of developing a sector-specific NCS.

Nesting

Focusing on a single sector immediately raises the issue of "nesting" — determining how the sector-specific cyber strategy and its implementation will fit simultaneously within the NCS and the strategy for the sector. In this case, determining how would developing and implementing a maritime cybersecurity strategy nest within and advance the NCS and, provided they have been developed, the *National Maritime Security Strategy* (focusing on the maritime security interests of the state) and/or *National Maritime Strategy* (including the security, governance, and economic activity of the state's maritime domain). In addition to considering the sector-specific strategy as it aligns with the NCS, there is the question of whether there are any relevant regional strategies. Understanding the applicable strategic work that has already occurred is a critical first step for a sectoral cybersecurity strategy. A misaligned or even poorly aligned strategy for the cyber concerns of one sector will breed confusion and create opportunities that criminal and nefarious actors can leverage.

Sectoral Stakeholders

Equipped with a clear understanding of the wider strategic context, the next step is to work on the "who" – identifying the sectoral-specific stakeholders. The maritime domain provides an excellent example of how important this phase is, as assumptions can be dangerous; there are almost always more

stakeholders than initially imagined. The stakeholders in the maritime space are decidedly different from those on land, but they are closely tied to land-based issues and interests, further emphasizing how important the nesting of sectoral work is. Furthermore, in identifying the stakeholders, we also begin to recognize that the sectoral threats are decidedly distinct yet can have a wider impact.

Some stakeholders are obvious. In any given country, the Navy, Coast Guard, or marine police will have a critical role in the conversation. So, too, will the maritime administration, port authority, fisheries ministry, and immigration and customs. Beyond that, however, we start to recognize that more actors have a stake in the maritime sector and the cybersecurity concerns around it than are initially obvious.

Shipping, oil and gas, mining, renewable energy, floating and offshore storage, dredging and fishing companies all have a critical stake in maritime cybersecurity, as do the government agencies that oversee and regulate them. Cruise lines, recreational boating, diving, and coastal tourism businesses, including hotels and resorts, are equally critical stakeholders in this space, along with their governmental oversight. So are marine biologists, fisheries and oceanography researchers, coastal communities, and fishing communities. And, while this list is by no means exhaustive, the vital stakeholders that no coastal, island, or archipelagic state can overlook are the owners, operators, and maintenance firms for the submarine cables that connect a country to the Internet and make cyber activity possible in the first place.

Cooperative Process

Addressing cybersecurity issues in the maritime domain usually requires an interagency response and often an international one. Furthermore, it almost always involves both public and private actors working, at a minimum, in a coordinated fashion, if not a fully integrated, collaborative one. While different sectors will have different considerations, these dynamics are often true, regardless of the sector. In order to bring the stakeholders together to articulate and implement a maritime cybersecurity strategy, it is critical to develop some form of process for collective action. This process begins as the mechanism for drafting the sector-specific cybersecurity strategy but can then evolve into being a more permanent fixture for handling the cybersecurity challenges.

No two country's processes will look exactly alike, nor will any two sectors be identical, but effective processes will all abide by certain principles. The stakeholders should articulate those principles at the outset to help shape the process. There are many examples of such multistakeholder efforts in different contexts like the World Privacy Forum and the US Maritime Operational Threat Response (MOTR) Process, each of which articulates different country and sector-specific principles. Generally, however, there are a few universal principles which should guide the process, regardless of the specific circumstances. The process must:

1. Be inclusive;
2. Be repeatable;
3. Be documentable;
4. Provide timely information to key decision-makers; and
5. Designate a clear lead agency.

This last point is critical, particularly for public-private and international engagement, as there needs to be a clear point of contact to serve as the conduit to the stakeholders outside of the government. If, for example, a ship's navigational system has been spoofed, as has occurred in the Black Sea, the Persian Gulf, and elsewhere, there is not time to have a debate or even a lengthy discussion as to who the lead agency and the main point of contact should be. Navigational spoofing could lead to collisions or other accidents that cause catastrophic environmental harm and loss of life, or significant economic harm as the Ever Given has shown. It does not matter who that lead agency is, so long as they are clearly designated and able to include all the other relevant stakeholders in a repeatable, documentable fashion that gets the right information to the right decision makers as quickly as possible.

Assessing the Sector

Once the stakeholders in the sector have been identified and a cooperative process established, the question becomes: what is their stake? In other words – what cybersecurity threats do they face and what capacity do they have to counter them? This is the transitional question that leads to the sector-specific assessments.

While it is focused on maritime security broadly – not maritime cybersecurity specifically – the *Africa Center for Strategic Studies*' Toolkit for strategy development breaks this assessment process into three parts: a self-assessment, a domain assessment, and a threat assessment.

For each of these assessments, the Toolkit poses a series of questions. Perhaps unsurprisingly, those questions parallel many of the areas of focus of the various cybersecurity frameworks discussed earlier in this paper.

Self-Assessment

Fundamental to developing and implementing any effective strategy is understanding the roles and responsibilities of the stakeholders who fall under it. A list of maritime stakeholders is therefore not enough. What stake do stakeholders actually have when it comes to maritime cybersecurity? What capacity already exists within the sector to identify cybersecurity threats? What laws are already on the books that could be leveraged? Where are there gaps? Who has investigative capacity? Who has law enforcement authority? This honest assessment of the capacity, capability, authority, jurisdiction and legal framework to address the sector's cyber issues is a critical first step – it is impossible to know where you need to go if you don't first know where you are. A 2020 publication with NATO's Maritime Interdiction Operations Training Center on "Making Maritime Strategy Work: A New Taxonomy" helps clarify and articulate the importance of this assessment, both for the development of strategy, and for the successful implementation of it.

Domain Assessment

A foundational principle of any type of security requires knowing what needs to be secured. Knowing what exists and why it is worth protecting helps shape a sector's approach to cybersecurity. In the maritime domain, most stakeholders will not be fully conscious of the full spectrum of maritime activities and their significance. For example, even some cyber professionals are unaware of the global reliance on submarine cables to the point that as of 2021, roughly 97% of all telephonic and Internet activity traverses the 420 privately owned submarine cables that sit on the ocean floor. They are the physical infrastructure that allows the cyberworld to continue developing, and during the COVID-19 pandemic, they have become even more critical. Maritime cybersecurity strategies that do not also include a national resilience plan for submarine cable protection, therefore, are not adequately addressing the domain. UNODC's Global Maritime Crime Programme is offering technical assistance for any country that requests it on this niche area submarine cable protection. But equally, matters like offshore energy infrastructure, seabed mining, or even something like an underwater tourism site need to be considered when examining cybersecurity concerns around which to build a maritime cybersecurity strategy. Regardless of the sector, a full appraisal of the domain, its value, and its vulnerabilities is critical.

Threat Assessment

Only with an understanding of the national capacity, capability, authority, jurisdiction and legal framework, and a good picture of the sector's attributes and why they are worth protecting, can a threat assessment really proceed. It is important, however, to note that while cybersecurity is the focus, attacks are not the only threats to digital continuity. Beyond the physical severing of a submarine cable, for example, weather can be a major factor in the maritime domain. So, threats need to look at the physical security of cyber-significant infrastructure as well as the cyber-specific threats.

In the maritime space, there are a few categories of threats to examine. All of the following are real examples of things that have happened in the maritime domain. While not exhaustive, these categories include:

1. Fraud includes things like spear phishing where a false email to a specific officer in a shipping company might inspire them to pay a bond to allow a ship to cross a canal over a weekend, only to discover that the bond money has been stolen, and that the email was a fake.
2. Facilitation of Crime could be hacking a database management platform to make certain containers carrying drugs disappear from the system.
3. Targeted Attacks may involve, for example, spoofing the Global Navigation Satellite System to make a ship's navigational controls suddenly believe that it is miles inland at an airport when it is clearly out at sea.
4. Theft of Data could include backdoor or ransomware attacks of a shipping company that might compromise the entire computing system of the company or steal sensitive information about vessels, cargo, or seafarers.
5. Operational Attacks can occur on either the information technology (IT) or operational technology (OT) of a ship and affect anything from rudder control to propulsion to ballasting to fuel meters, greatly impacting the movement and functioning of a vessel.
6. Broad Attacks may not be directed toward the maritime sector. Still, they may have tremendous impact on it like a virus that infects a shipping company's entire network and demands hundreds of millions of dollars in cryptocurrency to restore operations.
7. Human Error could be as simple as using an unsecured shoreside Wi-Fi network to log onto the Internet from a ship, only to result in the ship's systems being infected with malware.
8. Physical Attack could be as extreme as divers intentionally trying to cut a submarine cable with bolt cutters, but it could also involve fishermen accidentally cutting a cable while tied up to an offshore rig.
9. Technology Concerns grow by the day in the maritime space but involve everything from ship-to-shore drones to unmanned underwater systems to fully autonomous vessels.

Increased reliance on technology in the maritime sector – for navigation, detection of problems and even watchkeeping functions – means that there are new vulnerabilities that states need to know about and incorporate into national maritime cybersecurity strategies.

Part of assessing threats is not just about assessing the threat to the technology, but also the country. For example, now having seen the impact of the Ever Given, it is easier to understand that the main threat of an attack on the OT of a single vessel while traversing a canal is not so much to the ship itself as it is to the national and global economies.

Developing an Achievable Vision

Once the assessments are complete, the process of developing and drafting a strategy can proceed. The ultimate goal is crafting a vision that is actually achievable. For example, "ensuring that the country's maritime domain is free from cyber vulnerability" is an unrealistic end. Vulnerabilities will always exist, so the point is to ensure that mechanisms and processes are in place to adequately identify the vulnerabilities and collectively mitigate them in the first place, and then respond appropriately and effectively when those vulnerabilities are exploited.

In looking at the United States' *National Maritime Cybersecurity Plan*, for example, achievability was clearly a driving factor. The Plan is broken into three parts: Risks and Standards; Information & Intelligence Sharing; and Creating a Maritime Cybersecurity Workforce. While each of these three pillars have ambitious goals within them, this is not tantamount to "solving all maritime cybersecurity problems." Rather it is an achievable, actionable, implementable set of objectives, simply and clearly articulated, to ensure the continual improvement of cybersecurity in the maritime domain.

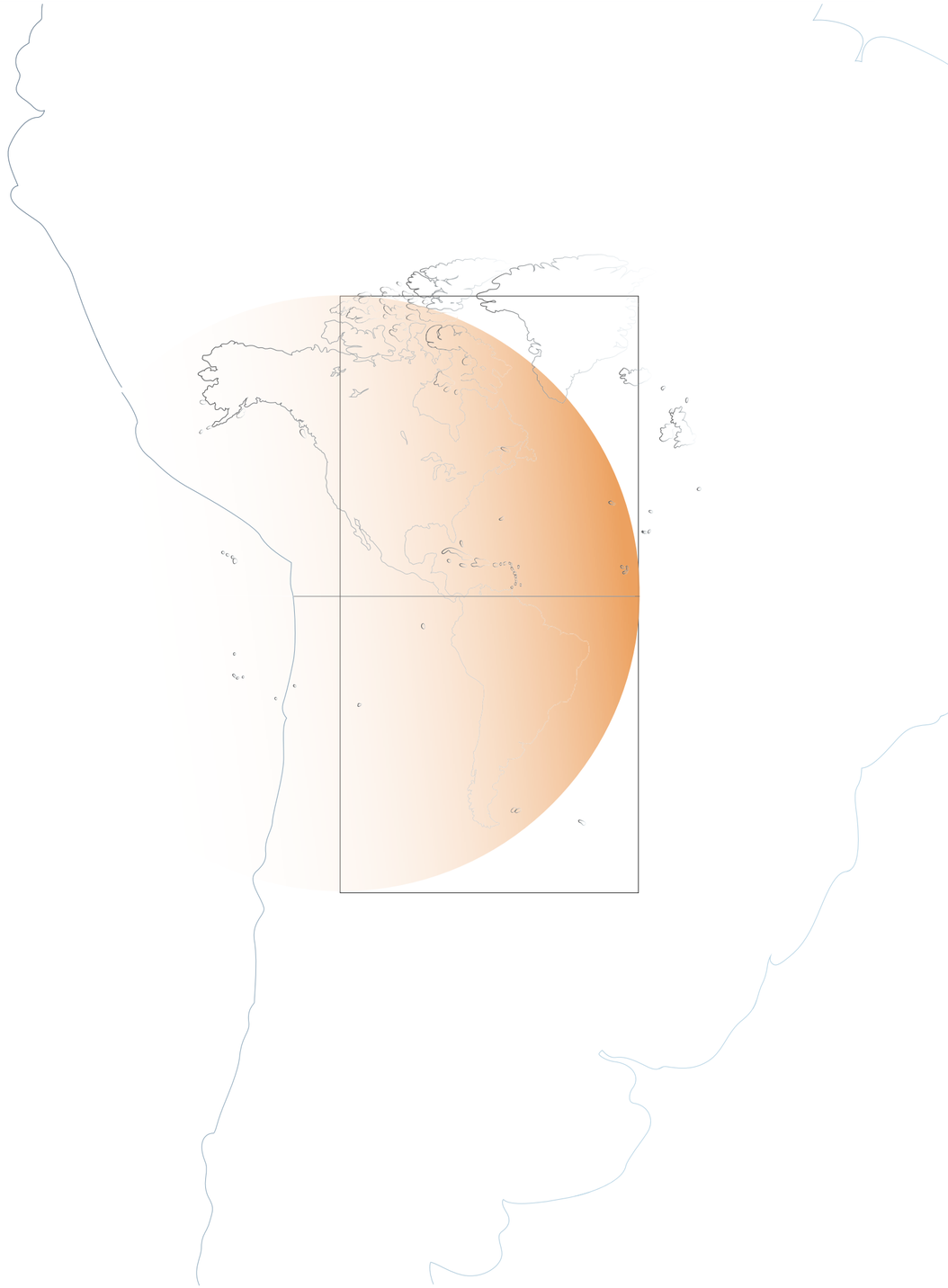
The maritime sector is becoming much more technologically advanced. As offshore infrastructure – particularly renewable infrastructure – develops and seabed mining and extractive processes become more sophisticated, cyber concerns grow. Too often, however, there is no public-private dialogue on what

the cyber concerns really are, nor are there proactive discussions about how to mitigate them. Only with a functional cooperative process between the stakeholders can a realistic and impactful vision be developed for how to manage this evolving space. Any sector should be conscious of cyber trends and what can be done collectively to secure the space, not just in the present, but also in the future.

Implementing the Vision

The cyber world is always changing. That is true of any sector. The maritime sector is always changing, as well. Amid a doubly turbulent environment, therefore, the implementation of the NCS at the sectoral level comes down to cooperation and agility. Can the stakeholders work together to adapt their approach to implementing the vision in light of changing circumstances? This is why having a sectoral-focused cybersecurity strategy nested within other related national strategies can help create the independence of movement needed to adapt at the sectoral level.

Ultimately, the point is not to be set to a dogma, a rigid guide, or a fixed set of rules, but to always remain mindful of mutually agreed foundational principles to help shape decisions in confronting the clash between the cyber sector and other critical sectors. Agility, creativity, resilience, continuity, and cooperation are all useful principles in this process. But in the end, the abiding principle for sectoral cybersecurity is simple: it has to work.



Notes

98 "Dominican Republic's Constitution of 2015," Constitute, last modified August 26, 2021, 86, https://www.constituteproject.org/constitution/Dominican_Republic_2015.pdf?lang=en.

99 "Cyber attacks in Latin America," Security News Desk Americas, July 3, 2020, https://snd-americas.com/cyber-attacks-latin-america/.

100 Inter-American Development Bank and the Organization of American States, Cybersecurity: Are We Ready in Latin America and the Caribbean? (2016), https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean.

101 Inter-American Development Bank and the Organization of American States, Cybersecurity: Risks, Progress, and the Way Forward in Latin America and the Caribbean, (2020), https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf.

102 Isabela Jibilian and Katie Canales, "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal." Insider, April 15, 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

103 "F.B.I. Identifies Group Behind Pipeline Hack," The New York Times, May 10, 2021, https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html.

104 K. Oanh Ha, Javier Blas, Mirette Magdy, Ann Koh, "How a Desert Wind Blew $10 Billion of Global Trade Off Course," Bloomberg, March 27, 2021, https://www.bloomberg.com/news/articles/2021-03-27/how-a-desert-wind-in-suez-canal-blew-global-trade-off-course.

105 Joe Weiss, "Was the Ever Given hacked in the Suez Canal?" Control, April 13, 2021, https://www.controlglobal.com/blogs/unfettered/was-the-ever-given-hacked-in-the-suez-canal/.

106 Ian Ralby, "Making Maritime Strategy Work – A New Taxonomy," NMIOTC, Issue 20, (2020): p 17-21, https://nmiotc.nato.int/wp-content/uploads/2020/08/NMIOTC-JOURNAL-20-2020-A.pdf.

107 World Privacy Forum, "Principles for Multi-Stakeholder Process (NTIA)," February 23, 2012, https://www.worldprivacyforum.org/2012/02/principles-for-multi-stakeholder-process/; Joseph Direnzo III and Christopher Doane, "The MOTR Process – Ensuring Unity of Effort in Maritime Security," Preparedness, February 28, 2007, https://www.domesticpreparedness.com/preparedness/the-motr-process-ensuring-unity-of-effort-in-maritime-security/.

108 Michael Jones, "Spoofing in the Black Sea: What really happened?" GPS World, October 11, 2017, https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/; and Michelle Weise Bockmann, "Seized UK tanker likely 'spoofed' by Iran," Lloyds List, August 16, 2019, https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran.

109 Africa Center for Strategic Studies, National Maritime Security Strategy Toolkit, (2016), https://africacenter.org/toolkit/national-maritime-security-strategy-toolkit/.

110 Ralby, "Making Maritime Strategy Work."

111 "Maritime Crime" United Nations Office on Drugs and Crime, accessed April 22, 2022, https://www.unodc.org/unodc/en/piracy/index.html.

112 United States. White House Office, National Maritime Cybersecurity Plan to the National Strategy for Maritime Security, (December 2020), https://www.hsdl.org/?abstract&did=848704.

CONCLUSION

As highlighted previously, there is no single way to develop an NCS. It is crucial that any strategy development process takes into account the unique national context, including its political, social, and economic landscapes, its needs, and its opportunities. However, there is value in sharing takeaways, good practices, and examples from NCS development in different countries. These can be adapted and replicated regionally. International organizations like the Global Forum on Cyber Expertise provide a useful space for stakeholders to share experiences in conducting cybersecurity efforts on the ground.

Below are some key takeaways and examples from countries outside of the Americas that can be useful for policymakers in the process of developing their NCS.

Maximizing sustainability and stakeholder buy-in (including opposition leaders) can help foster validation and adoption

It will be key to ensure that the strategy has the support of all stakeholders before moving to formal adoption. This can take place in a variety of ways, one of them is through a "validation" workshop or through other means that provides a final confirmation and endorsement of the NCS as a whole before it is forwarded to the appropriate responsible agency or body. A validation workshop can be an effective way to build trust and ensure stakeholder buy-in.

Validation Workshop Example: Ghana

In Ghana, a validation workshop was held before adopting the first Ghanaian National Cybersecurity Policy and Strategy (NCPS) in 2015. It gathered representatives from different stakeholder groups to discuss priorities for its future implementation. This final validation from stakeholders was seen as essential to ensure broader community buy-in, and to the legitimacy of the development process itself. Since then, Ghana has reviewed its National Cybersecurity Policy and Strategy under the leadership of the National Cybersecurity Centre, which convened different workshops to gather stakeholder input, including an open forum in October 2019 during Ghana's Cybersecurity Month, where the revised draft was again presented for stakeholder input.

The roadmap should be holistic, tailored to the local context, and enhance transparency and accountability

For a roadmap to be successful, it should have a holistic stakeholder engagement plan as piecemeal multistakeholder approaches can only be partially successful. If relevant stakeholders are only invited to comment on the NCS in the later stages of drafting or are only involved in the initial stages but not involved in its implementation, then the value of stakeholder engagement is far from being fully realized and there will be a missed opportunity for building trust, a key element in the NCS implementation

As well as engaging with stakeholders through the process of developing the NCS, it is important that the NCS itself reflects the same commitment to multistakeholder approaches in the way it will be implemented and evaluated.

In addition to the roadmap being holistic, it is important that it sets out clearly defined and transparent procedures and mechanisms. Being clear on roles and responsibilities and rules of engagement from the very beginning will ensure that each stakeholder has clarity with regard to at which subsequent stages they'll be called upon, and how they'll be expected to contribute to the process. Making documents available on the right channels and in a timely fashion will allow stakeholders to engage meaningfully.

Some recommendations to ensure transparency and accountability include:

- Ensuring there's clarity of stakeholder interests and affiliations;
- Developing clear procedures and mechanisms (for example, clear procedures for the inclusion and exclusion of stakeholder input, clear decision-making powers and mechanism, mechanisms for accountability and redress.);
- Ensuring there are records management systems such as documenting and publicly disclosing discussions and decisions; and
- Ensuring the existence of lines of accountability: was the leadership accountable to the group as a whole? Were stakeholders accountable to the group as a whole?

Australia's NCS 2020

In August 2020, the Australian government released Australia's Cybersecurity Strategy 2020, the successor to its 2016 NCS. As part of the strategy development, a series of consultations were convened. Having a structured plan for consultations can be seen as a way to increase clarity and transparency over the mechanisms to gather stakeholder input. Between September 2019 and February 2020, the government met with over 1,400 people from across the country in face-to-face consultations, including workshops, roundtables, and bilateral meetings. 215 written submissions were received in response to their call for views. 156 of these submissions were public and have been published, contributing to the process being transparent but also allowing submissions to stay confidential when stakeholders requested it.[113] The Minister for Home Affairs also established an Industry Advisory Panel to provide strategic advice to support the development of the Australian Cybersecurity Strategy 2020.

Countries should practice continued assessment and develop iterative processes that should continue even after the adoption of their strategy.

The policy and strategy development process is not linear. Some or all steps may be repeated several times. For example, there may be more than one opportunity for inputs, and two or more rounds of drafting and review, particularly given the range of policies and mechanisms that are core to cybersecurity strategies. Once the NCS is adopted, the process does not end there. As we saw in Part Four of this document, ongoing evaluation will be key to revise the NCS considering learnings from its implementation.

Example: Norway

Norway was one of the first countries to develop an NCS in 2003 and, so far, has developed four strategies. The government decided to develop a strategy after an independent committee, looking into all national vulnerabilities, identified cybersecurity as an emerging critical issue. In 2015, another independent committee reported on Norway's digital vulnerabilities. In 2017, the Ministry of Justice and Public Security followed this with their first white paper on cybersecurity, which paved the way for a national strategy update in 2018. [114]

Notes

113 "Submissions and Discussion Papers," Australian Government Department of Home Affairs, accessed April 22, 2022, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020.

114 Global Forum for Cyber Expertise, *National Strategies: Interviews Behind the Cover*, (GFCE, 2018), https://thegfce.org/wp-content/uploads/2020/09/GFCE-2018-National-Strategies-small.pdf. Global Forum for Cyber Expertise, National Strategies: Interviews Behind the Cover, (GFCE, 2018), https://thegfce.org/wp-content/uploads/2020/09/GFCE-2018-National-Strategies-small.pdf.

FINAL **WORDS**

Understanding how critical cybersecurity is to national strategy is the first step towards improving cybersecurity for all members and levels of society. Starting with an assessment is critical; as mentioned earlier in this paper, it is impossible to know where you need to go if you don't first know where you are. The tools, guides, examples, and case studies offered in this paper are your starting point. The final results must be guided by the unique characteristics of every state.

ANNEXES

Annex A: **DESIGN THINKING AND THE "ROOTS & FRUITS" EXERCISE**

The "Roots & Fruits" (see Figure 5) is adapted from Gamestorming – A Playbook for Innovators, Rulebreakers and Changemakers, by D. Gray, S. Brown, & J. Macanufo (2010) and Four.[115] A seemingly simplistic depiction, it offers an approach to the sequencing prioritization effort described in Part Four by providing a visual model for the relationship between dependent activities. In this exercise, the fruits represent the desired goals or objectives, the trunk represents ways (initiatives or activities) to reach the objectives, and the roots depict those foundational activities or functions that must be in place to enable them, such as legislation, policy, popular support, resources, or effective governance structures. The planning team starts at the top, with strategic goals. Then for each goal, they identify the initiatives, programs, or actions they will employ to achieve them. Finally, for each of these initiatives or activities, they will note any conditions that must be in place for them to succeed. For example, if one of a country's goals is protection of its critical infrastructure and services, a key implementing initiative might be to establish cyber-security standards for those sectors. Some enabling conditions for that initiative may include formally identifying critical infrastructure and services in law, establishing the legal authorities to regulate them and delineating which entities will have that role, and allocating sufficient resources to assist operators in implementing the standards selected. Once these dependencies are identified, the team may find that certain initiatives cannot reasonably be implemented within the current strategy cycle simply because the pre-requisite activities themselves will require substantial time and effort—this is particularly common where laws or governing processes must be established first. In this case, the team may choose to focus the current strategy cycle on establishing those foundational elements, saving the dependent activities for the next implementation cycle. To ensure that those future activities stay on the radar, it's a good idea to document the projected long-term strategic path, as described in Part Four, and reconsider dependent initiatives or programs once their "roots" are in place.

"Roots and fruits" Exercise

Grow this three from top to bottom

- What are our strategic goals or objectives? **(Fruit)**
- How do we reach goals? **(Trunk)**
- What is required to enable and sustain them (Such as foundations in law, governance, political support, resources, etc,)? **(Roots)** Some roots support many fruits...

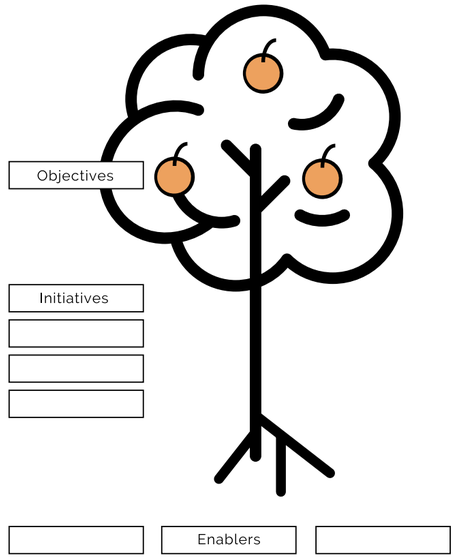


Figure 5 **Roots and Fruits Exercise**[116]

Desired Ends - National Goals or Objectives (Fruits)

Example: developing secure e-services, improving incident response, securing critical infrastructure, or combatting cybercrime.

Ways to Achieve Goals (Trunk)

Example: Law enforcement and judicial training programs are enabling capabilities for tackling cybercrime; information sharing partnerships support incident response.

Means of Enabling (Roots)

Example: legislative structure for cyber property and privacy is a foundation for combatting cybercrime; a regulatory structure supports protection of critical infrastructure.

Annex B: **DESIGN THINKING APPROACH TO RETURN-ON-INVESTMENT PRIORITIZATION**

Like the sequencing activity, the exercise presented below is adapted from Gray, Brown, and Macanufo's Gamestorming – A Playbook for Innovators, Rulebreakers and Changemakers (2010). It is useful for prioritizing initiatives or activities (as opposed to things, like critical infrastructure sectors or facilities), because it is focused on impact.

In this approach, multistakeholder teams are again assembled. If the number of initiatives to be considered is manageable, a single team may be able to do the entire exercise. If the number is too big, it is possible to create separate teams to address each high level goal/objective, and the proposed implementation initiatives or activities associated with it. This approach can be used for any goal or objective that has more than a handful of initiatives associated with it, and it is particularly useful where there are 6-20 proposed activities. [NOTE: This method is most effective when it is facilitated by some objective party because it works best when participants must work through the exercise one step at a time, without knowing what comes next — otherwise there is a natural human inclination to cheat by manipulating the early analysis steps.

Once the team(s) are convened, they should be provided the full list of initiatives they are to consider. It is helpful if the initiatives can be referred to by shorthand or a nickname because the facilitator will use a sticky note for each one, but at the same time, the participants should have the full description to refer to. It is also helpful to have someone familiar with each proposed initiative in the room to explain and advocate for it, and to be able to inform other stakeholders about any benefits, constraints, complexities, or other key considerations, that may not be apparent to those less familiar with the functional area it addresses.

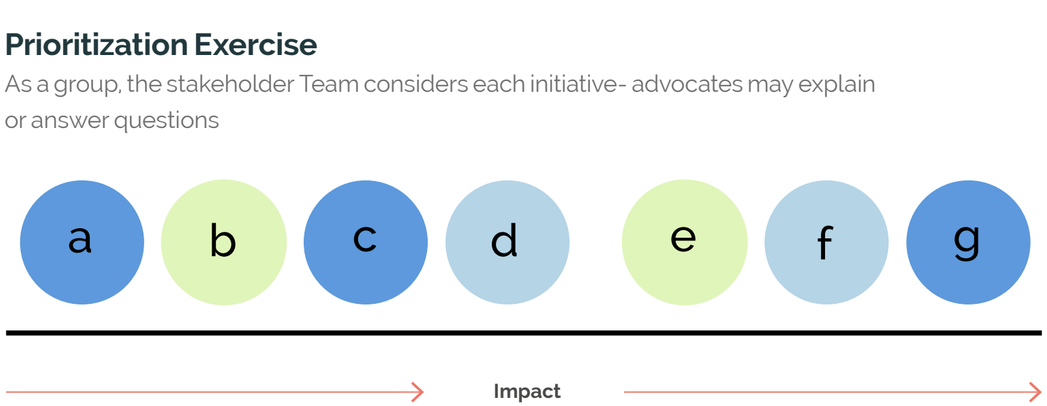
Before getting started, it is important that the group spend some time reviewing and agreeing to a few basics:

- Participants in the exercise should agree to interact as equals in the discussion, regardless of the size or influence of the organization or function they represent, their seniority, or job title. If undue influence is exerted, the prioritization will not truly reflect the needs of the country or organization/function it is intended to support;
- Stay focused on the current step—do not look ahead to next steps or try to revise the output of previous steps; and
- Review the higher goal(s) or objective(s) the initiatives under consideration are intended to address. Consider the risks that are being addressed, or the opportunities achieved—the 'why' of the effort. This is important in determining how and to what degree the initiatives under consideration are relevant and impactful.

Once everyone is on board, they can settle into the hard work of prioritization. The method that follows is illustrated in its entirety in the figure below (right), but as mentioned above, it is most effective when only the facilitator knows the whole process.

Step 1: Stakeholder participants consider all the initiatives associated with a particular Goal/Objective one by one, arranging them along a straight line from least impactful to most impactful. It is very important that in making this determination, they should be directed to imagine the initiative is being implemented in a perfect world, where feasibility is no issue and only the best-case impact is relevant. There can be no "ties"—everything must be arranged linearly. This step is typically contentious: it may take an hour or more for an average sized group to deal with a list of fewer than 10 proposals, and collegial argument is to be expected and welcomed. The facilitator should emphasize that placing one idea below another does not mean that it is not important, but only that it has less theoretical impact in achieving the goal. Allow discussions to continue until a reasonable consensus is achieved on the order of impact/effectiveness

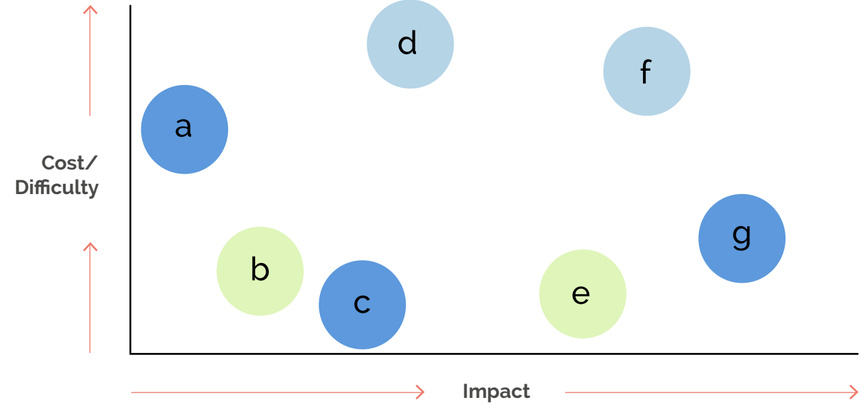
Figure 6 **Demonstrating the Prioritization Exercise**[117]



- Entire Stakeholder Group collectively arranges all of the initiatives in increasing order of "perfect world" potential **effectiveness** in achieving strategic goals. Do not consider feasibility, just impact

NOTE: If the same team is going to prioritize the initiatives under more than one goal/objective, repeat this step for all goals/objectives before moving on to Step 2.

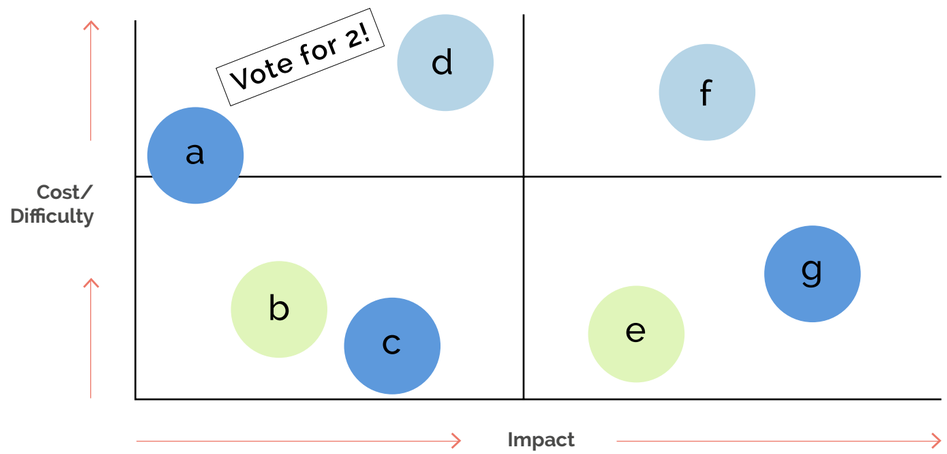
Step 2: This is where the discussion moves from the "perfect world" to the "real world." Without changing the order of the sticky notes, participants should adjust them vertically (along a notional y-axis) according to difficulty. "Difficulty" can represent cost, time, complexity, scale, the human resources required, political considerations, or anything else that might affect the initiative owner's ability to implement it. The higher the sticky note is raised, the harder, more complex or costly it is. This step is usually less contentious, and the subject matter experts can be very informative about potential barriers. At the end of this step, the group's list of initiatives under consideration will still be arrayed in the same order of effectiveness, but arranged at various heights on the board (NOTE: although it is not optimal, in situations where groups cannot convene in person, it is possible to use remote tools such as the Mural application to accomplish the exercise virtually, although it is much harder to see the whole picture at once that way).



- With initiatives remaining in the same order, the group elevates each other along the y-axis according to **difficulty**, which may mean cost, complexity, time, expertise, political barriers, etc.

As with Step 1, if the same group is prioritizing initiatives under more than one goal/objective, they should complete this step for all goals/objectives before continuing.

Step 3: Keeping the arrangement of the initiatives intact, the facilitator adds a simple grid (see Figure 6) that divides the set into equal quadrants. The facilitator labels each quadrant as Luxury (High Cost/Difficulty, Low Impact), Quick Win (Low impact, but Cheap/Easy), Investment (High Cost/Difficulty but High Impact), and High ROI (Affordable/Achievable, High Impact). This characterization is the reason it is important that they not know how the exercise will proceed in advance—no one wants an initiative that they favor to end up in the Luxury category!



- Once the group has reached consensus, the Facilitator adds quadrants to differentiate solutions as Luxury, Quick Win, Investment, or High ROI

Luxury: Low Impact and Difficult/Costly
Quick Win: Low Impact, but Cheap/Easy
Investment: Expensive/Difficult, but Impactful
High ROI: Affordable/Feasible and High Impact

Each participant votes for two-initiatives with the most votes are selected, up to the number deemed executable (typically 18-25 over 5 years)

Step 4: Each participant gets two votes (a smaller, different color sticky note, or dots, or pins, or similar can be used), which they can use however they wish—to vote twice for something they feel strongly about, or to vote for two different priorities, such as one Quick Win and one High ROI. Initiatives in the Luxury quadrant rarely get a significant number of votes and are thereby effectively eliminated. High ROI items will usually receive the most votes, with the remainder being split between various Quick Win and Investment initiatives. Usually, but not always, there will be clear winners in each of these categories, which garner a significantly larger number of votes.

Repeat the quadrant/vote step for each goal/objective. At the end of this effort, the number of initiatives under serious consideration is typically somewhat reduced by the elimination of low feasibility/low impact items, and other priorities will have emerged. Occasionally, something that is clearly important, such as critical infrastructure protection or workforce development, will end up in the "Luxury" quadrant. This is usually because more than half of the other initiatives under consideration were viewed by participants as being more immediately impactful. During the voting phase, these initiatives may garner numerous votes, which will help highlight the discrepancy, and which the group can use its discretion to resolve through discussion. Sometimes, however, there really are other activities the stakeholders feel are more impactful and achievable. Again, this should be a matter for follow-on discussion, as there may be good reason to push these initiatives

to a later cycle. For example, a country with a low cyber threat context and infrastructure that is still largely disconnected from the Internet may consider advancing its digital government services to be more important in the near term than implementing critical infrastructure cyber-security standards. Remember, the point of prioritization is not to determine what is important to do, but simply to determine what is important to do first. Facilitators should keep a tally of the votes each initiative received (this can be done by taking a photo of the board) in case an additional step is needed to narrow down the final list, as described below.

The final step is, of course, applying these outcomes to facilitate implementation. This is where our quadrants pay off:

- Those items identified as offering a High ROI (high impact and affordable or achievable) can be easily separated out to form the core of the implementation plan.
- Quick Wins can be considered separately, outside the strategy process. Because they are inherently cheap/easy, but also represent comparatively lower gains, they can be implemented when convenient—immediately to gain symbolic momentum, or later in conjunction with higher priority related initiatives, to demonstrate commitment to a program even if it was not prioritized high enough for full implementation, or later in the strategy cycle if additional resources become available.
- Strategic Investments are more expensive or difficult, but high impact. In most cases, countries cannot afford to do more than one or two of these in a particular implementation cycle. Deciding which to select may depend on the factors discussed in step 4: which ones take a long time or are essential to enabling future activities? These should be the top contenders in this area. And by agreeing to push the others in this quadrant to a later cycle, planners can free up resources and expertise to be applied to high-ROI initiatives.
- Luxury initiatives can be eliminated or shelved for later consideration.
- Some groups, having played by the rules to arrive at this prioritization, may find that in the course of discussion they identified commonalities that might allow two or more initiatives to be combined into one program—as long as the consolidation is reasonable according to the participants, this should be encouraged, since it keeps more good ideas in the mix. Investment initiatives will be addressed in greater depth below.

Remember: the goal should be a total of no more than 25 or so initiatives (the example below uses 20) across all Strategic Goals. If each team identified two strategic investments and four or five high-ROI initiatives for each of six goals (as an example), that still leaves implementers with 36-42 initiatives competing for resources. How should the stakeholder team decide which ones to focus on?

If necessary, decision-makers should be able to draw a line based purely on votes, since those will almost certainly encompass at least the highest ROI initiatives. It is often the case that natural "break points" arise. To identify these, the team should list all the High ROI items in order of the number of votes received (this is where those photos of the vote tallies come in handy) and draw a line at number 25, as shown in the figure below. Looking at that line, does it fall such that the item or two right below it got very nearly as many votes as the one above? Or, alternatively, is there a big drop-off in the number of votes several items above where the line fell? These are natural breakpoints and show where priorities are almost equal. In general, or if resources are extremely constrained, move up the list to the nearest breakpoint. Some High ROI initiatives will be pushed to the next strategy cycle, but the ones that remain will be more likely to have the resources and attention needed for execution. If everything above the line is extremely high priority, and the next breakpoint below it is close and significant, consider including those near-equivalent items. However, be aware in this case that more hard decisions may be needed later in the cycle if resources prove insufficient or new, unanticipated needs arise (new, unanticipated needs almost always arise over the course of a strategy cycle!). It may be possible to take the lowest group of the selected items and identify portions of each that can be executed with confidence, holding other phases in reserve to implement if feasible.

Figure 7 **ROI and Prioritization**[118]

High ROI IN	Votes
Initiative 1	29
Initiative 2	28
Initiative 3	28
Initiative 4	27
Initiative 5	26
Initiative 6	23
Initiative 7	17
Initiative 8	17
Initiative 9	16
Initiative 10	15
Initiative 11	15
Initiative 12	14
Initiative 13	14
Initiative 14	14
Initiative 15	13
Initiative 16	9
Initiative 17	8
Initiative 18	8
Initiative 19	8
Initiative 20	8
Initiative 21	8
Initiative 22	8
Initiative 23	4
Initiative 24	3

Natural breakpoint

Move cutline up to the next natural breakpoint if resources are constrained or the next breakpoint is far below the cut-line

Pre-determined Cut Point

Move cutline down if the next natural breakpoint is sufficiently close, resources are adequate, or value is very high

Annex C: **KEY OBJECTIVES AND LINES OF ACTION - CARIBBEAN REGION**

Legal and Regulatory Frameworks

Variables	Dominican Republic	Jamaica	Trinidad & Tobago
Legislation			
Legislative Frameworks for ICT Security			
Human Rights Online		X	
Data Protection Legislation			
Intellectual Property Legislation			X
Cybercrime Legislation		X	X
Publication of Technical Standards	X		
Review Existing Legislation		X	X
Critical Infrastructure Law			
Defense and Cyber-security			
Criminal Justice System	X	X	X
Prosecution	X	X	X
Law enforcement	X	X	X
Reporting Mechanisms	X	X	X
Cooperation to Combat Cybercrime		X	

Cybersecurity Culture

Variables	Dominican Republic	Jamaica	Trinidad & Tobago
Public Awareness Raising			
National Campaigns			
Sector Specific Campaigns	X	X	X
Multistakeholder Initiatives	X	X	X
Cybersecurity Mind-set		X	
Trust on Online Services/Commerce	X	X	X
Personal Information Protection Online			

Multistakeholder Engagement

Variables	Dominican Republic	Jamaica	Trinidad & Tobago
Public Sector			
Standards/Guidelines		X	X
Information Sharing			
Coordination and Cooperation	X		X

Multistakeholder Engagement

Variables	Dominican Republic	Jamaica	Trinidad & Tobago
Capacity Building			
Domestic Industry Development			
Private Sector			
Information Sharing Arrangements		X	X
Critical Infrastructure	X	X	
Capacity Building		X	X
Public-Private Partnerships		X	
International Relations			
Information Exchange	X	X	X
Multilateral Cooperation Agreements	X	X	
Combating Criminal Activities	X	X	X
Capacity Building		X	
Convention on Cybercrime			

Technical Capability/Capacity-Building

Variables	Dominican Republic	Jamaica	Trinidad & Tobago
Incident Response			
Establishment of a National CSIRT	X	X	X
CSIRT Capacity at the National Level			
Identification and Management of Incidents		X	X
Information Sharing with Various sectors	X	X	X
Reporting Mechanisms			
Establishment of Sectoral CSIRTs	X		
Critical Infrastructure Protection			
Identification	X		X
Risk Management/Assessment/Profile	X	X	X
Adherence to Standards	X	X	X
Public-Private Partnership	X	X	
Education, Research and Training			
Academic Programs	X	X	X
Professional Training	X	X	X
Public-Private Partnerships	X	X	X

Annex D: **KEY OBJECTIVES AND LINES OF ACTION – CENTRAL AMERICA REGION**

Legal and Regulatory Frameworks

Variables	Belize	Costa Rica	Guatemala	Mexico	Panama
Legislation					
Legislative Frameworks for ICT Security					
Human Rights Online					
Data Protection Legislation			X		X
Intellectual Property Legislation					
Cybercrime Legislation	X		X		
Publication of Technical Standards			X		
Review Existing Legislation	X	X		X	
Critical Infrastructure Law		X	X	X	
Defense and Cyber-security					
Criminal Justice System	X	X	X	X	X
Prosecution	X		X	X	X
Law Enforcement	X	X	X	X	X
Reporting Mechanisms	X	X			X
Cooperation to Combat Cybercrime		X	X		

Cybersecurity Culture

Variables	Belize	Costa Rica	Guatemala	Mexico	Panama
Public Awareness Raising					
National Campaigns	X	X	X		X
Sector Specific Campaigns	X	X	X		
Multistakeholder Initiatives	X	X	X		
Cybersecurity Mind-set	X	X			X
Trust on Online Services/ Commerce			X	X	
Personal Information Protection Online					

Multistakeholder Engagement

Variables	Belize	Costa Rica	Guatemala	Mexico	Panama
Public Sector					
Standards/Guidelines		X	X		X
Information Sharing		X		X	
Coordination and Cooperation			X		

Multistakeholder Engagement

Variables	Belize	Costa Rica	Guatemala	Mexico	Panama
Capacity Building		X	X		
Domestic Industry Development				X	X
Private Sector					
Information Sharing Arrangements	X	X		X	
Critical Infrastructure		X			
Capacity Building		X	X		
Public-Private Partnerships		X			
International Relations					
Information Exchange	X		X		
Multilateral Cooperation Agreements	X		X		
Combating Criminal Activities	X		X		
Capacity Building	X	X			
Convention on Cybercrime	X	X	X		X

Technical Capability/Capacity-Building

Variables	Belize	Costa Rica	Guatemala	Mexico	Panama
Incident Response					
Establishment of a National CSIRT	X		X		
CSIRT Capacity at the National Level	X	X		X	X
Identification and Management of Incidents				X	
Information Sharing with Various Sectors	X		X		
Reporting Mechanisms	X				
Establishment of Sectoral CSIRTs	X	X	X		X
Critical Infrastructure Protection					
Identification	X	X	X		
Risk Management/Assessment/ Profile	X	X			X
Adherence to Standards	X	X	X		X
Public-Private Partnership		X	X		
Education, Research and Training					
Academic Programs	X	X	X	X	X
Professional Training	X	X	X		X
Public-Private Partnerships		X			X

Annex E: **KEY OBJECTIVES AND LINES OF ACTION – SOUTH AMERICA REGION**

Legal and Regulatory Frameworks

Variables	Argentina	Brazil	Chile	Colombia	Ecuador	Paraguay
Legislation						
Legislative Frameworks for ICT Security			X			
Human Rights Online						
Data Protection Legislation			X			
Intellectual Property Legislation						
Cybercrime Legislation		X				X
Publication of Technical Standards						
Review Existing Legislation	X	X	X	X	X	X
Critical Infrastructure Law					X	
Defense and Cyber-security						
Criminal Justice System						X
Prosecution	X		X		X	X
Law enforcement					X	X
Reporting Mechanisms	X		X		X	X
Cooperation to Combat Cybercrime					X	

Cybersecurity Culture

Variables	Argentina	Brazil	Chile	Colombia	Ecuador	Paraguay
Public Awareness Raising						
National Campaigns	X		X	X	X	X
Sector Specific Campaigns		X	X	X	X	X
Multistakeholder Initiatives	X		X			
Cybersecurity Mind-set					X	X
Trust on Online Services/ Commerce						X
Personal Information Protection Online		X				

Multistakeholder Engagement

Variables	Argentina	Brazil	Chile	Colombia	Ecuador	Paraguay
Public Sector						
Standards/Guidelines		X	X	X		X
Information Sharing			X			X
Coordination and Cooperation	X				X	X
Capacity Building	X		X	X	X	

Multistakeholder Engagement

Variables	Argentina	Brazil	Chile	Colombia	Ecuador	Paraguay
Domestic Industry Development	X	X	X			X
Private Sector						
Information Sharing Arrangements		X		X	X	
Critical Infrastructure	X		X		X	
Capacity Building		X		X		X
Public-Private Partnerships				X	X	
International Relations						
Information Exchange		X	X	X		
Multilateral Cooperation Agreements	X	X	X		X	
Combating Criminal Activities						
Capacity Building			X			
Convention on Cybercrime			X		X	

Technical Capability/Capacity-Building

Variables	Argentina	Brazil	Chile	Colombia	Ecuador	Paraguay
Incident Response						
Establishment of a National CSIRT			X			
CSIRT Capacity at the National Level		X		X	X	X
Identification and Management of Incidents				X		X
Information Sharing with Various Sectors	X		X	X		X
Reporting Mechanisms			X		X	X
Establishment of Sectoral CSIRTs		X	X	X	X	X
Critical Infrastructure Protection						
Identification	X		X		X	X
Risk Management/Assessment/ Profile	X	X	X		X	X
Adherence to Standards		X	X	X	X	X
Public-Private Partnership	X	X	X		X	
Education, Research and Training						
Academic Programs	X	X	X	X	X	X
Professional Training	X	X	X	X		X
Public-Private Partnerships	X	X				X

Annex F: **AT A GLANCE: MATURITY ASSESSMENT TOOLS**

TOOL	PURPOSE	AUDIENCE	KEY PILLARS	METHOD
Combating Cybercrime Capacity Building Assessment Tool **The World Bank**	To determine gaps in capacity building and highlight priority areas to direct capacity building resources	Policymakers, Legislators, Law Enforcement authorities, civil society	• Non-Legal Framework • Legal Framework • Procedural Law • e-Evidence • Jurisdiction • Safeguards • International Cooperation • Capacity Building	Entirely self-administered - requires no tracking, ranking, or reporting back of results
Cyber Readiness Index 2.0 (CRI) **The Potomac Institute for Policy Studies**	To evaluate and measure a country's preparedness levels for cybersecurity risks.	Global leaders, National and Regional governments, Ministries, government agencies, academia, cybersecurity experts and researchers	• National Strategy • Incident Response • E-crime and law enforcement • Information sharing • Investment in R&D, Education and Capacity • Diplomacy and Trade • Defense and Crisis Response • Defense and Crisis Response	Not self-administered - tool is applied by team of experts from the CRI team
Cybersecurity Capacity Maturity Model for Nations (CMM) **Global Cybersecurity Capacity Centre (GCSCC)**	To benchmark a country's cybersecurity capacity and enable nations to self-assess, plan investments and national cybersecurity strategies, and set capacity	Governments - The data is used to produce a report ranking the country's maturity level (start-up, formative, established, strategic, or dynamic) and submitted to the	• Cybersecurity Policy and Strategy • Cyber Culture and Society • Cybersecurity Education, Training and Skills • Legal and Regulatory Frameworks	Member State responses to the GCI questionnaire are verified by the ITU GCI team, and weighted on recommendations from an expert weightage group. Member States' responses are used to

TOOL	PURPOSE	AUDIENCE	KEY PILLARS	METHOD
	development priorities	government with recommendations.	• Standards, Organizations, and Technologies	create cybersecurity profiles
National Cybersecurity Index (NCSI) **e-Governance Academy (eGA)**	NCSI is a global index used to provide an overview of current issues affecting the cyber realm worldwide	Country Ministries/ Agencies, Cybersecurity agencies/ policymakers, Academia, Cybersecurity experts	• Cybersecurity Policy Development • Cyber Threat Analysis and Information • Education and Professional Development • Contribution to Global Cybersecurity • Protection of Digital Services • Protection of Essential Services • E-Identification and Trust Services • Protection of Personal Data • Cyber Incident Response • Cyber Crisis Management • Fight Against Cybercrime • Military Cyber Operations	Data is collected from government officials, organizations, or individuals and the NCSI conducts public data collection. Data is then reviewed by NCSI experts and published on the NCSI website.
National Cybersecurity Strategies Evaluation Tool **ENISA**	To help member states evaluate strategic priorities and objectives related to National Cybersecurity Strategies	European Union Member States	• National cyber contingency plans • Protection critical information infrastructure	Interested country completes a 30-minute online evaluation

TOOL	PURPOSE	AUDIENCE	KEY PILLARS	METHOD
			• Organize cybersecurity exercises • Establish baseline security measures • Establish incident reporting mechanisms • Raise user awareness • Foster R & D • Strengthen training and educational programs • Establish an incident response capability • Address Cybercrime • Engage in international cooperation • Establish public-private partnerships • Balance security with privacy • Institutionalize cooperation between public agencies • Provide incentives for private sector to invest in security measures	
National Cybersecurity Framework Manual	Sets out the 5 national cybersecurity dilemmas that nations have to deal with to	States or any interested individuals	• Stimulate the Economy vs. Improve National Security	

TOOL	PURPOSE	AUDIENCE	KEY PILLARS	METHOD
	deal with to achieve a safe and secure cyberspace		• Infrastructure modernization vs. Critical Infrastructure Protection • Private Sector vs. Public Sector • Data Protection vs. Information Sharing • Freedom of Expression vs. Political Stability	

Annex G: **AT A GLANCE: NCS GUIDES**

GUIDE	PURPOSE	AUDIENCE	SCOPE
Guide to Developing a National Cybersecurity Strategy, 2nd Edition	To provide a set of principles and good practices on the development, establishment and implementation of national cybersecurity strategies.	Any interested individual	• NCS Development process • NCS Lifecycle • initiation, stocktaking and analysis, production, implementation, reviews • Focus Areas / Key Elements to Include • Governance; Risk management in national cybersecurity; Preparedness and resilience; Critical infrastructure and essential services; Capability and capacity building and awareness raising; Legislation and regulation; and International cooperation • Cross-cutting Considerations • vision; comprehensive approach and tailored priorities, inclusiveness, economic and social prosperity, fundamental human rights, risk management and resilience, appropriate set of policy instruments, clear leadership, roles and resource allocation, trust environment

GUIDE	PURPOSE	AUDIENCE	SCOPE
National Cybersecurity Strategy Good Practices Guide - ENISA	To help member states leverage ICTS For socio-economic development	CTO Members	• Introduction and background • Guiding principles • Vision and strategic • Objectives and priorities – using a risk-based approach • Stakeholder section • Governance and management structure • Strategy implementation, including legal and regulatory frameworks, capacity building, awareness, local technical capability, and incident response • Monitoring and evaluation
Commonwealth Approach for Developing National Cybersecurity Strategies - CTO	To provide steps, objectives and good practices and analyses of NCS in the EU and EFTA area	EU Member States and EFTA Countries	Outlines NCS lifecycle and provide examples of good practice
Developing a National Cybersecurity Strategy - Microsoft	To provide recommendations for developing or improving and national cybersecurity strategy	Policymakers	• Explains what a cybersecurity strategy is and outlines foundational principles as the basis for a national strategy (risk based, outcome focused, prioritized, practicable, respectful of privacy and civil liberties, and globally relevant).

Annex H: **AT A GLANCE: INVOLVING STAKEHOLDERS IN NATIONAL CYBERSECURITY STRATEGIES: A GUIDE FOR POLICYMAKERS**

Why involve stakeholders?	Better informed and evidence-based policy outcomes: Cybersecurity affects a range of stakeholders, all with unique experiences and perspectives. Bringing this expertise will produce a more accurate and evidence-based picture of the cybersecurity landscape and possible implications of policies. More effective implementation of the NCSS: Almost all NCSS contain public-private partnerships so involving stakeholders in the development process ensures stakeholder buy-in and enables more effective implementation.
Who are relevant stakeholders?	Broadly speaking, all stakeholders are relevant when it comes to cybersecurity, because everyone has an interest in ensuring a free, open, and secure cyberspace. But when it comes to cybersecurity policymaking more specifically, relevant stakeholders tend to refer to: • Those with a mandate, role, or responsibility in the process; • Those with skills or expertise needed to inform the policy and operationalize it, and • Those who could be disproportionately affected by the policy or its implementation. Examples include government departments, other public bodies e.g., telecommunications regulators, academic institutions, civil society organizations, international and regional organizations, the technical community including the incident response community, and the private sector.
How to involve stakeholders at each stage of the NCSS Lifecycle	Stage 1: Initiation • Stakeholder engagement can range from formal to informal, with governments consulting stakeholders or alternatively governmental and non-governmental stakeholders may deliberate and make decisions on an equal footing. Stage 2: Stocktaking and Analysis • One cost-effective way of gathering stakeholders' input can be through online consultations and questionnaires. An alternative means to gather information is through in-person meetings or workshops which could be open or closed - with invitations only to particular stakeholders and actors. In-person meetings have the benefit of allowing dialogue between different participants, which is not feasible in an online consultation. Stage 3: Production of the NCSS • Employing the same engagement methods as the previous stage, stakeholders should be drawn upon to inform the structure, objectives, and priority areas of the NCSS. The drafting of the text is likely to be led by the authority or governance body, the structure of which could itself be multistakeholder, ensuring a more inclusive approach to drafting. • Once the NCSS draft is ready, stakeholders can be invited to review and comment on the text through a consultation - either online or in person. • Involving stakeholders in the NCSS validation before moving to formal adoption can be a way to effectively build trust and ensure stakeholder buy-in. Stage 4: Implementation • In the development of an implementation Action Plan, the precise roles of stakeholder groups should be determined. It is worth considering at this stage whether additional multistakeholder mechanisms should be established to coordinate, oversee, and implement the Action Plan or specific activities. Depending on the existing interest and capacity of local stakeholders, additional investment and efforts might be necessary to facilitate meaningful stakeholder at this stage. Stage 5: Monitoring and Evaluation • Mirroring the modalities of engagement outlined in stage 2, Stakeholders should be able to provide information necessary to evaluate the overall success of the NCSS; the extent to which it has met its goals and objectives; and help identify whether any revisions are needed.
Tips for successful stakeholder engagement	• To be most effective, stakeholders should be engaged in a holistic and sustained way. • Conducting a comprehensive mapping of the stakeholder landscape at the beginning of the process and undertaking specific assessments at each stage of the NCSS lifecycle is also invaluable. This will help with identifying levels of cybersecurity awareness among stakeholders and where additional skills and expertise is needed. • Transparency and communication are key and it is crucial to share the NCSS roadmap with stakeholders and be clear on roles, responsibilities, and rules of engagement.

Notes

115 Design Thinking exercises adapted from: D. Gray, S. Brown, and J. Macanufo, Gamestorming – A playbook for innovators, rulebreakers and changemakers, (Sebastopol, CA: O'Reilly Media Inc, 2010) http://gamestorming.com/impact-effort-matrix-2/.

116 Figure by the MITRE Corporation and used with permission.

117 Figure by the MITRE Corporation and used with permission.

118 Figure by the MITRE Corporation and used with permission.

National Cybersecurity Strategies:

Lessons Learned and Reflections from the Americas and Other Regions

OAS More rights for more people

GLOBAL PARTNERS DIGITAL