Multistakeholder Approaches to National Cybersecurity Strategy Development

GLOBAL PARTNERS DIGITAL

June 2018

Contents

This report is authored by Matthew Shears, Daniela Schnidrig, and Lea Kaspar. The authors wish to thank all contributors who have read and commented on earlier versions of this report.

The development of this report was made possible with support from the Foreign & Commonwealth Office of the United Kingdom.

Published in London 2018 by Global Partners Digital.

About this report

For some time, governments and non-governmental actors alike have been calling for greater stakeholder involvement in cybersecurity policy. Despite this, multistakeholder approaches to national cybersecurity strategy (NCSS) development remain comparatively rare.

In part, this is as a result of a critical gap in the cyber capacity building landscape, which currently offers few (if any) resources to support and guide the implementation of such approaches. This report seeks to address the gap.

- **Section 1** outlines existing guidance models for developing NCSSs.
- **Section 2** looks at the development of NCSSs in four target countries – Chile, Ghana, Kenya and Mexico – with the aim of exploring different approaches and extracting lessons learned. It explores how stakeholder engagement is reflected across the three stages of NCSS development – scoping, formation, and drafting. As the examples seek to demonstrate, when multistakeholder approaches are applied in a comprehensive and structured way they can result in more informed and effective cybersecurity strategies, policies and governance, greater stakeholder engagement, and, ultimately, greater support and buy-in for the NCSS and its implementation.
- In **Section 3**, the report sets out a blueprint for developing a NCSS in a multistakeholder manner based on the good practices identified through the four examples, and provides the basis for the development of more comprehensive, stakeholder-driven cybersecurity strategies.

Introduction

Inclusive or multistakeholder approaches to policymaking are not new. They have been tested and applied in a range of policy spaces, including climate change, extractive industries, conflict prevention, and peace building, among others[1]. In the internet governance space, the Internet Assigned Numbers Authority (IANA) transition – which, in 2016, saw the United States Government transfer its clerical and stewardship roles in the Domain Name System to the multistakeholder community – was seen as proof that multistakeholder approaches can address difficult and challenging policy issues and produce credible and workable solutions.

One area where such approaches have obvious value is in the development of national cybersecurity strategies (NCSSs), which are now widely seen as critical to a nation's economic and social well-being. The cybersecurity challenges that a nation faces are broad and interrelated. This, in turn, necessitates an approach that leverages a broad set of expertise and engages a diverse set of stakeholders in the NCSS development process.

In the field of cybersecurity policy, the need for effective cross-stakeholder collaboration is now widely recognised, with numerous international instruments reinforcing the message. The Global Conference on CyberSpace (GCCS) (also known as the London Process),[2] has highlighted the need for multistakeholder engagement and cooperative approaches to cybersecurity challenges, with the 2013 Seoul Framework calling for "a trusted, secure and sustainable environment in partnership with multiple stakeholders, including international organizations and the private sector"[3], and the 2015 Chair's Statement urging governments "to ensure that cyber policy at the national, regional and international level is developed through multistakeholder approaches."[4] Similarly, a 2015 report by the United Nations Group of Governmental Experts suggests that effective responses to cyber security challenges "would benefit from the appropriate participation of the private sector, academia and civil society";[5] while the Commonwealth, in Principle 1 of its Commonwealth Cybergovernance Model,[6] stated: "We contribute to a safe and an effective global Cyberspace as a partnership between public and private sectors, civil society and users, a collective creation; with multi-stakeholder, transparent and collaborative governance promoting continuous development of Cyberspace;... (and through) enabling and promoting multi-stakeholder partnerships."

These high level commitments are reflected in a number of NCSSs explored in this report. For example, the Ghanaian government's cybersecurity strategy states that there is a need to address fully "all aspects of cyber security, especially the multi-stakeholder approach to fighting the cyber menace"[7] and the Mexican government's cybersecurity strategy states that "Success of the strategy will depend on stakeholder collaboration"[8] and that "Mexico's national cybersecurity strategy is a live document that will set the roadmap for the development of cybersecurity in Mexico, with an integral, transversal and holistic approach and with the collaboration of different stakeholders."[9] However, examples of implementing the approach remain scarce, and practical guidance lacking.

The aim of this report is to support efforts to involve relevant stakeholders in the process of developing NCSSs by capturing existing examples of good practice and providing practical guidance based on these examples. In doing so, the report draws upon Global Partners Digital (GPD)'s extensive work on multistakeholder processes,[10] NCSS guidance models, as well as good practices and lessons learned from inclusive approaches to the development of NCSSs in Chile, Ghana, Kenya, and Mexico. While outside the scope of this report, its authors recommend further comparative research to identify and capture examples of NCSS development from other countries. Additionally, this research could easily be extended to capture examples of stakeholder engagement in the processes of NCSS implementation and evaluation.

[1] See, for example, Hemmati, M., *Multi-stakeholder Processes for Governance and Sustainability*, 2002, Earthscan. Other initiatives are outlined here: http://www.mspguide.org/case-studies.

[2] See GPD's GCCS Info Hub at gp-digital.org

[3] GCCS, *Seoul Framework for and Commitment to Open and Secure Cyberspace*, 2013

[4] GCCS, *Chair's Statement*, 2015.

[5] United Nations General Assembly, *Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2016

[6] Commonwealth ICT Ministers Forum, C*ommonwealth Cybergovernance Model*, 2014

[7] p.6, Ghana, *National Cyber Security Policy and Strategy*

[8] p 4, Mexico, *National Cybersecurity Strategy* (Estrategia Nacional de Ciberseguridad), quote translated by GPD

[9] p.24, Ibid

[10] GPD, *Framework for Multistakeholder Cyber Policy Development* (2018). Download at gp-digital.org/publications/framework

01
Existing guidance models

The importance of engaging stakeholders in cybersecurity strategy development and implementation is enshrined in a variety of NCSS models, guides and approaches adopted by various organisations, including the International Telecommunication Union[1] and the Organization of American States (OAS)[2], among others. This report draws on three documents in particular: The Commonwealth Approach for Developing National Cybersecurity Strategies,[3] the European Union Agency for Network and Information Security (ENISA) National Cyber Security Strategy Good Practices Guide,[4] and the University of Oxford's Cybersecurity Capacity Maturity Model for Nations (CMM).[5] In each of these, the role of stakeholders is highlighted, and their involvement seen as a critical factor in both the development of a NCSS and the overall cyber-readiness of a nation.

The Commonwealth Approach for developing National Cybersecurity Strategies highlights the importance of working with stakeholders when developing NCSSs:

> *... due to the nature of Cybersecurity, it is also imperative that the National Cybersecurity strategy is developed in a multi-stakeholder partnership that brings together the public sector, private sector, academia and the civil society while also drawing on the knowledge, expertise and competencies of the international community ... The exercise of developing the strategy will also benefit those participating stakeholders by improving their awareness and mutual understanding of the disparate opportunities, risks, needs and capabilities of the different stakeholders. Reflecting the global and connected nature of Cyberspace, these stakeholders may be national and international bodies, both regional and global, both public and private sector plus civil society.*[6]

The ENISA NCSS Good Practice Guide highlights the importance of engaging with and involving stakeholders. A number of the national NCSSs reviewed by ENISA in the report noted the importance of engaging stakeholders, leading ENISA to recommend that stakeholders be involved sooner rather than later in the development of a NCSS:

> *Recommendation 6: Approach and involve stakeholders at an early stage of development - Certain EU Member States were successful in increasing the willingness of private actors for future collaboration by approaching them at an early stage of development of their NCSS, new laws or measures. When drafting new legislation or developing a new or updated NCSS, it is recommended to engage private stakeholders at an early stage of the process.*[7]

The government of Malta's cybersecurity strategy – reviewed by ENISA while compiling its cybersecurity guidance document – notes that "The pervasive nature of cyber space essentially calls for a multi-stakeholder approach towards its security."[8]

The University of Oxford's Cybersecurity Capacity Maturity Model for Nations (CMM)[9] is designed to measure the cyber-readiness and cyber-capacity of a state and has been used by numerous countries and by regional entities to assess and promote the adoption of cybersecurity frameworks, institutional responses, and appropriate policy and legal measures. Throughout the CMM there is mention of the role of stakeholders and multistakeholder engagement across the model's maturity levels.

Although the importance of stakeholder engagement is highlighted in all three documents, none offer any structured guidance to help design a NCSS development process in a multistakeholder way. This report aims to address this lack of practical guidance and seeks to build on and complement existing guidance models. In doing so, the authors hope to inform and strengthen future iterations of the above documents.

[1] E.g. ITU, *National Cyber Security Strategy Guide*

[2] Inter-American Development Bank (IDB); Organization of American States, *Cybersecurity: Are We Ready in Latin America and the Caribbean?*, 2016

[3] *Commonwealth Approach for Developing National Cybersecurity Strategies*, revised 2015

[4] ENISA, *NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies*, November 2016

[5] Global Cyber Capacity Building Centre, *Cybersecurity Capacity Maturity Model for Nations (CMM)*

[6] p.5, *Commonwealth Approach for Developing National Cybersecurity Strategies*, Revised 2015

[7] p.53, ENISA, KPMG, "Interview questionnaire: Austria"; ENISA, KPMG: "Interview questionnaire: Malta". Both in ENISA, *NCSS Good Practice Guide:Designing and Implementing National Cyber Security Strategies*, 2016

[8] p.11, Malta, *National Cyber Security Strategy Green Paper*

[9] Global Cyber Capacity Building Centre, *Cybersecurity Capacity Maturity Model for Nations (CMM)*

02
Good practice examples

While multistakeholder approaches to cyber policy development have been widely endorsed in principle, the number of cybersecurity-related processes being conducted in a multistakeholder manner remains low.

There are many possible reasons for this – including perceptions around cost and complexity, a lack of understanding of potential benefits, and, perhaps most crucially, a general sense of simply not knowing where to start.

As with any new process or mechanism, there will be learning curves and associated costs. This said, the only real additional substantive consideration relates to involving stakeholders and the mechanisms needed to ensure that their views are taken into account. Any additional costs of bringing stakeholders together in a multistakeholder setting to discuss cybersecurity will likely be offset by the overall benefit of having a strategy or policy outcome that is more effective, impactful, and has greater buy-in from the outset. Below, we look in more detail at the incorporation of multistakeholder approaches in four country case studies.

Two other practical challenges arise. The first, as mentioned above, is the paucity of practical guidance on how to apply multistakeholder approaches to the development of a NCSS. The the second is the lack of use cases that illustrate the benefits of multistakeholder approaches.

This chapter aims to address the latter challenge by capturing examples of efforts to involve stakeholders in the development of national cybersecurity strategies (NCSSs) in four countries – Chile, Ghana, Kenya and Mexico. To do this, the report employs an analytical framework based on GPD's work on multistakeholder approaches[1] and the different NCSS guidance models referenced above, and reviews stakeholder engagement in target countries across the three stages of the NCSS development cycle – from **scoping**, through **process formation**, to the NCSS **drafting stage**.[2]

Stage 1: Scoping

This stage is all about assessing existing cybersecurity capabilities and resources: identifying gaps in cyber capabilities; defining critical infrastructure; assessing levels of threat; reviewing cybersecurity strategy and policy frameworks already in place; and consulting existing best practice and model NCSSs to extract relevant learnings.

The first step is to gain a full and accurate understanding of the relevant country's cyber landscape. This can be done through using a cybersecurity readiness or maturity model such as the Cybersecurity Capacity Maturity Model (CMM)[3]. As the Commonwealth suggests, "a maturity model can indicate where a country lacks intrinsic capacity in aspects of Cybersecurity [...] Those capacities may be needed to reduce risks to national goals or to create opportunities for the country. For example, a maturity model might offer a measure of a country's Cybersecurity legal frameworks. Weaknesses in that framework for example may mean that the country must invest there first in order to make any progress."[4]

In Ghana, a cybersecurity capacity maturity review was undertaken in the first quarter of 2018 using the abovementioned CMM. Its aim was to gain a more in-depth understanding of Ghana's cybersecurity capacity and to identify areas for further investment based on an analysis of data collected through the model's application.[5] Engaging stakeholders during the review was singled out by the Deputy Minister for Communications as an important factor in its success, and that involving cybersecurity experts in such initiatives is key to assessing, measuring and evaluating a country's cybersecurity readiness.

[1] GPD, *Framework for Multistakeholder Cyber Policy Development* (2018). Download at gp-digital.org/publications/framework

[2] Typically, a NCSS will also comprise implementation and evaluation stages in which the strategy is put into practice and its impact assessed. While these stages can and do in many cases include stakeholders in a variety of roles, they are outside the scope of this report.

[3] Global Cyber Capacity Building Centre, *Cybersecurity Capacity Maturity Model for Nations (CMM)*

[4] p.7, *Commonwealth Approach for Developing National Cybersecurity Strategies*, revised 2015

[5] Ghanaian Ministry of Communications, "Cybersecurity Capacity Maturity Model Assessment held," 2018

Stakeholders can be involved more fully through, for example, the creation of a multistakeholder committee (or similar body) to collaborate on the scoping stage work. In the initial stages of the development of Mexico's NCSS, 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 NCSS.[6]

As the ENISA report suggests, bringing in stakeholders at an early stage is recommended. This sentiment is echoed in the Commonwealth's approach to NCSSs, which suggests that both the "design and delivery of the strategy should include a wide range of stakeholders from across the public and private sectors, across academia and drawn from civil society."[7] Involving relevant stakeholders in the Scoping Stage – or the "design" of the strategy as the Commonwealth calls it – allows for a more comprehensive assessment of the cyber-readiness of a nation.

Characteristics of a multistakeholder approach

For the purpose of this report, we define the multistakeholder approach through the four characteristics that are central to ensuring effective stakeholder engagement, as identified in GPD's Framework for Multistakeholder Cyber Policy Development.[8]

1. **Open and accessible**: The degree to which opportunities for relevant stakeholder engagement – through participating in committees, workshops, drafting sessions, consultations, etc. – are communicated in a timely manner via relevant channels, and efforts made to address any obstacles that may prevent or discourage participation

2. **Inclusive of stakeholders' views:** The extent to which relevant stakeholders are given the opportunity to contribute, different views and interests of those stakeholders are heard, considered and accounted for, inputs are published, and deliberations are informed and evidence-based.

3. **Consensus-driven**: The degree to which stakeholders can agree ways forward and find common purpose.

4. **Transparent and accountable**: The extent to which procedures and mechanisms are clearly defined and transparent. Factors considered in this characteristic include disclosure of stakeholder interests and affiliations, clarity and effectiveness of lines of internal accountability, and mechanisms for ensuring discussions and decisions are fully documented.

While the extent to which certain characteristics are applied may differ depending on the specificities of the process in question, each plays a key role in supporting effective stakeholder engagement in NCSS development. A more open process is likely to facilitate a more informed dialogue in which the participating stakeholders contribute their views and expertise. This dialogue in turn helps build trust between stakeholders, a key prerequisite for collaboration and consensus-driven decisionmaking. And a commitment to transparency and accountability builds confidence in the strategy development process and trust in its eventual outcome and implementation

[6] OAS Technical Assistance Mission, "Recommendations for the Development of the National Cybersecurity Strategy", 2017

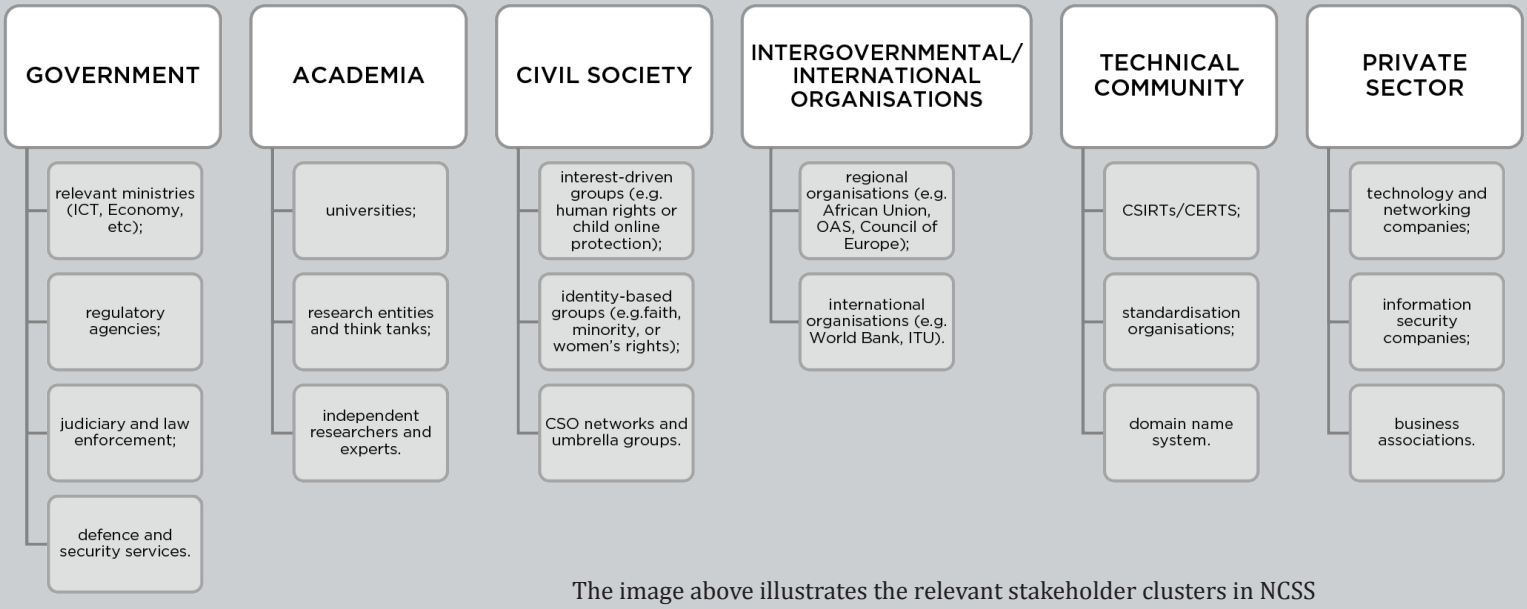
[7] p.15, *Commonwealth Approach for Developing National Cybersecurity Strategies*, revised 2015.

[8] More detailed descriptions for each characteristic can be found in GPD, *Framework for Multistakeholder Cyber Policy Development*.

Identifying "relevant stakeholders"

Not all stakeholders need to be involved in every discussion. Relevant stakeholders are those with a direct interest and expertise in the issue at hand, who can contribute credible and constructive input and engagement to the process. At the same time, governments need to be wary of applying unnecessarily restrictive approaches to stakeholder engagement.

Given the wide-ranging impacts that cybersecurity threats can have across economy and society, a multiplicity of views will need to be accounted for in the development of a NCSS. Relevant stakeholders in the case of NCSS development may include: various government ministries/agencies; law enforcement; security services; private sector actors, particularly critical information infrastructure owners, tech companies, and information security companies; the technical community for CERT/CSIRTS, standards, protocols and networking; civil society, academia, and independent experts working on a broad spectrum of issues including human rights, governance and the societal impact of cyberattacks. Bringing these varied but important relevant stakeholders to the table is critical.



The image above illustrates the relevant stakeholder clusters in NCSS development, including a non-exhaustive list of potential stakeholders under each cluster.[9]

Any stakeholder clustering should be approached with flexibility and caution, as categories and subcategories may need to differ depending on the process in question, the local context, and stakeholder self-identification. In some cases, categories or subcategories may overlap. As a rule of thumb, the framework for identifying relevant stakeholders should be as broad and flexible as needed so that it does not restrict effective participation by relevant actors.

[9] Based on stakeholder participation in NCSS development in Chile, Ghana, Kenya, and Mexico.

Stage 2: Formation

During this stage, the vision, goals and objectives are established, along with the structures and processes that will be used to achieve those goals and deliver the NCSS. These structures and processes would typically include: governance and management structures; information sharing processes; institutional and regulatory frameworks; roles and responsibilities; mechanisms for involving stakeholders; and rules of engagement. This stage is also where the broad focus of the NCSS is determined – whether, for example, it will be a high level framework, or a detailed cybersecurity strategy with appropriately elaborated policies and practices.

Involving stakeholders in setting out the vision, scope, and objectives of the NCSS helps ensure greater overall stakeholder buy-in for the NCSS and its development. It also encourages a broader discussion, driven by a wider spectrum of relevant expertise. In a multistakeholder approach to developing a NCSS, agreeing the roles and responsibilities and operating parameters for the strategy development process is critical. The Commonwealth Approach for Developing National Cybersecurity Strategies provides a range of examples for establishing a vision and strategic goals, including issues as diverse as strengthening infrastructure, tackling cybercrime, among others.[10]

The Kenyan NCSS highlights the following objectives:

> *The Government of Kenya is committed to the safety, security, and prosperity of our nation and its partners. We see cybersecurity as a key component in that commitment, providing organizations and individuals with increased confidence in online and mobile transactions, encouraging greater foreign investment, and opening a broader set of trade opportunities within the global marketplace. Successful implementation of the strategy will further enable Kenya to achieve its economic and societal goals through a secure online environment for citizens, industry, and foreign partners to conduct business.*[11]

As we saw in the Scoping Stage, bringing together expert stakeholders in a committee structure (as was the case in the development of the Mexican NCSS) can be an effective tool in leveraging relevant local stakeholder expertise. Mexico's Technical Assistance Mission not only looked into the current state of cybersecurity in Mexico, but also advanced proposals for the construction and definition of a National Cyber Security Framework, effectively spanning both the Scoping and Formation Stages.

A similar vehicle was used in the early stages of the development of the Ghanaian NCSS, with a Multistakeholder Ad-hoc Technical Committee established by the Ministry of Communications to develop its policy and strategy. The Committee played a significant role in: defining the terms to be used; reviewing existing policy and laws to identify gaps; reviewing conventions and country specific policies and strategies (such as the Budapest Convention and the draft African Union Convention); and developing the strategy text. As with the Mexican committee, the Ghanaian committee spanned both the Scoping and Formation Stages.[12]

[10] Section 4, *Commonwealth Approach for Developing National Cybersecurity Strategies,* revised 2015

[11] p.4, Kenya, *National Cybersecurity Strategy*

[12] Ghanaian National Cybersecurity Policy and Strategy, presentation by Eric Akumiah.

Stage 3: Drafting

At this stage, the strategy or framework begins to take shape. The text is drafted and the component parts of the strategy and framework are agreed. The overall timeline and number of steps within this stage will depend on the scope of the NCSS, and the level of detail necessary to address the cybersecurity needs of the country in question. These needs may include developing cyber contingency planning and cyber incident response mechanisms and raising user awareness of cybersecurity issues, among others.

The types of relevant stakeholders included in the drafting will depend on the scope of the NCSS and the technical aspects that it covers. For example, a high level framework strategy – a typical starting place for governments seeking to put a NCSS in place – will not necessarily require technically oriented consultations or inputs. However, when establishing incident response mechanisms, setting up a CERT/CSIRT, or assessing infrastructure vulnerabilities, a greater degree of technical expertise will likely be necessary.

There is no single approach when it comes to structuring the drafting stage. Good practices will differ significantly, based on the scope of the NCSS, the range of stakeholders involved, the technical requirements, and other factors. Typical mechanisms to involve stakeholders could include committees, roundtables/ workshops, consultations, expert interviews, etc. These are neither mutually exclusive nor exhaustive. The drafting process benefits from being as open and inclusive as possible, so that the fullest expertise and representation can be brought to the development of the NCSS.

As part of the initial stages of the drafting process of the Chilean cybersecurity policy, the Inter-Ministerial Committee in charge of driving the process held meetings with relevant actors and stakeholders based on the five pillar structure of the NCSS.[13] In order to develop each pillar, the Committee held two meetings. In the first, it set out the work plan and main elements and objectives for the pillars, as well as implementation measures to achieve these objectives. In a second meeting, relevant actors and stakeholders were invited to give input, providing oral testimony and written submissions. These meetings with selected stakeholders were seen as a way to create dialogue, build buy-in and legitimacy, increase meaningful participation, and contribute to having evidence-based and informed deliberations.

However, for a drafting stage to be multistakeholder, relevant stakeholders should be involved throughout. The ability of stakeholders to access, participate in, and contribute to the drafting process is essential. For example, in the case of Ghana, once the Multistakeholder Ad-hoc Technical Committee had drafted the strategy, it was presented to local stakeholders for further review and comment. Further inputs were incorporated, and the final draft was revised and then forwarded on to the Ministry of Communications. Stakeholders were involved throughout, both from within the Committee itself and, more broadly, prior to the final draft being submitted.

[13] For more detail on the five pillars, see a document by the Chilean ministry of defence and internal security, *Bases para una politica nacional de ciberseguridad*, 2015.

In Chile, Kenya and Mexico, a draft of the NCSS was posted online, allowing stakeholders to submit comments. Having the opportunity to input on an online platform can make the process more accessible to those unable to participate in-person, and in turn more inclusive. Publishing the inputs received can make the process more transparent.[14] Publishing the strategy draft for comment is therefore clearly good practice in the development of NCSSs. However, it should be seen as a minimum requirement, rather than sufficient in itself.

An important complement to publishing the strategy draft for comment is holding public hearings involving stakeholders. When developing its national cybersecurity strategy, Mexico hosted a series of open workshops with national stakeholders with the aim of gathering input at different stages of the drafting process. One of these was a forum at the Senate, which convened representatives of the Executive and Legislative branches of the Mexican Government, as well as international experts who shared their countries' experience in the formation of NCSSs. A two-day workshop followed, in which the first draft of the national cybersecurity strategy was reviewed. Recommendations included a number of measures to involve additional stakeholder inputs, including a cybersecurity and human rights workshop organised jointly with the OAS/CICTE Cybersecurity Program.[15]

The final piece in the Drafting Stage is when the text is ready to be forwarded on to responsible party for the final review and adoption, typically a government agency. This last step in the drafting process can take place in a variety of ways. In the Ghanaian NCSS development process, for example, it happened through a stakeholder "validation workshop." This final moment of assent from stakeholders is seen as essential to broader community buy-in, and to the legitimacy of the development process itself.

It is important to note that NCSS drafting is not a linear process, and some or all steps in this stage 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. This said, it is important that the process be designed to move forward, and does not simply rehash the same discussions repeatedly.

General considerations

As the cases above illustrate, there is no one single "correct" model to involve stakeholders in the development of a NCSS. 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. In all cases, multistakeholder approaches to the development of the NCSS can pay dividends, as we've seen in the case studies mentioned above.

However, for such approaches to be successful and for the dividends of such approaches to be fully realised, a number of elements need to be in place.

The first prerequisite is for a genuine commitment from government, and indeed all stakeholders, to multistakeholder approaches and engagement in the development of the NCSS. Examples of good practice that could contribute to strengthening commitments to multistakeholder approaches include institutionalising commitments within government ministries and agencies, having actors within government and other

[14] Comments to the draft of the Chilean National Cybersecurity Policy can be accessed at: http://www.ciberseguridad.gob.cl/consulta-ciudadana/. Comments to the draft of the Mexican strategy can be accessed at: https://www.gob.mx/participa/consultas/documento-ciberseguridad

[15] Forum, "Towards a National Cybersecurity Strategy: Perspectives on Human Rights and Collaboration among Multiple Stakeholders," 2017

influential stakeholders champion the approach, or international endorsements or incentives. Seeking stakeholder engagement should not be a box-ticking exercise, but rather an approach that is expected to add significant value. This notion was explicitly highlighted in the stakeholder recommendations to the development of the Mexican NCSS, which noted that both the "formulation and implementation of the strategy should be the result of a multi-stakeholder engagement process."[16]

Another thing to consider is that piecemeal multistakeholder approaches can only be partially successful. In other words, if relevant stakeholders are only invited to comment on the NCSS in the later stages of drafting, or are only involved in the implementation of the NCSS (but were not invited to engage in the development process), then the value of stakeholder engagement is far from being fully realised.

The third, and perhaps most important condition for success is ongoing engagement. The commitment to engaging with stakeholders must be carried through the process of developing the NCSS so that, as much as possible, the final NCSS continues to reflect that same commitment to multistakeholder approaches in the way it is implemented and evaluated.

[16] OAS Technical Assistance Mission, "Recommendations for the Development of the National Cybersecurity Strategy", 2017

03
Recommendations

Building on the examples above, as well as existing NCSS guidance models, it is possible to distil a set of good practices that can bring about more comprehensive stakeholder engagement in the NCSS development process, and help foster buy-in and legitimacy around the strategy itself.

The following three elements can be understood as practical building blocks for implementing a multistakeholder approach to the development of a NCSS:

1. Establish a multistakeholder NCSS Committee

As a first step in considering developing a NCSS, the government should, from the outset, establish a multistakeholder NCSS Committee (as was the case for the development of the Mexican and Ghanaian NCSSs) or equivalent as the primary entity responsible for developing the NCSS. This committee should retain this role from the Scoping through the Drafting Stages to ensure continuity. This approach encourages a greater diversity of views, expertise, and inputs from relevant stakeholders from the outset, and can provide a more comprehensive perspective of the cyber landscape and the appropriate scope of the NCSS. Creating and empowering a multistakeholder NCSS Committee is an essential element in the "formulation and implementation" of the strategy, as noted above.

The Committee should also be responsible for ensuring transparency and accountability of the process. And, as far as is possible, the Committee should also operate on a consensus basis, working to ensure that there is common purpose and collaboration in fulfilling its responsibilities.

2. Ensure stakeholder and expert engagement on an ongoing basis

Throughout the development of the NCSS it is critical to ensure ongoing engagement, support, and contributions from stakeholders, particularly those not represented on or participating in the work of the Committee. To do so, the Committee should, at appropriate and regular milestones in the NCSS development process, build in the opportunity for regular input from stakeholders. This is key to meeting the multistakeholder characteristic of openness and accessibility, outlined in chapter 2.

As illustrated in the case studies from Chile, Ghana, Kenya, and Mexico, these opportunities could take the form of consultations, hearings or similar, workshops and/or roundtables, or targeted meetings with stakeholder experts on specific technical or security issues. The Committee should ensure that inputs from these stakeholder sessions are appropriately considered and accounted for. This would meet the characteristic of inclusivity of stakeholder views (again, see chapter 2).

The multistakeholder Committee should also call on additional representation and expertise when required, and ensure that it has the appropriate institutional relationships in place – both inside and outside government – along with related information-sharing protocols to ensure productive collaboration. Ongoing engagement with a range of cybersecurity-related experts, such as CSIRTs/CERTs, and critical infrastructure representatives, etc., is also essential.

3. Conclude the NCSS development process with multistakeholder validation of the strategy

While the work of the Committee could extend beyond the finalisation of the NCSS into implementation and evaluation, its last important act as part of the multistakeholder development of the NCSS will be to ensure that the strategy has the support of all stakeholders. This means giving stakeholders an opportunity to confirm and endorse the NCSS as a whole before it is forwarded by the Committee to the appropriate responsible agency or body. In the Ghanaian NCSS development process cited earlier in the report, this took the form of a "validation workshop"; depending on the specific process, a different format might be more appropriate.

*

We welcome feedback on this report, as well as use cases. In particular, if you have a real-life example of a multistakeholder approach to NCSS development you would like to share, please email info@gp-digital.org

GLOBAL PARTNERS DIGITAL

Second Home
68 Hanbury St
London E1 5JL

+44 203 818 3258