GFCE
Global Forum on Cyber Expertise

A Short Guide to Stakeholder Engagement on National Cybersecurity Strategy Development

GFCE Working Group A
Strategy & Assessments Task Force

March 2022

A short guide to stakeholder engagement for National Cybersecurity Strategy development

GFCE WG A - Task Force Strategy & Assessments

Authors

This guide has been developed under the umbrella of the Global Forum on Cyber Expertise (GFCE), Working Group A - Task Force Strategy and Assessments, as a project under its Work Plan 2021-22. The guide has been compiled by (in alphabetical order):

- Carolin Weisser Harris, Global Cyber Security Capacity Centre (GCSCC)
- Daniela Schnidrig, Global Partners Digital (GPD)
- Elizabeth Orembo, Global Cyber Security Capacity Centre (GCSCC)
- James Boorman, Oceania Cyber Security Centre (OCSC)
- Kerry-Ann Barrett, Organization of American States (OAS)

The information and views set out in this paper are those of the authors and do not necessarily reflect the official opinion or position of GFCE, its Secretariat or its members and partners. Neither GFCE nor its members may be held responsible for the use which may be made of the information contained therein.

About the GFCE

The GFCE was launched at the Global Conference on Cyber Space in The Hague based on the vision that everyone should be able to fully reap the benefits of Information and Communicate Technology (ICT) through a free, open, and secure digital world. The GFCE was tasked with a clear mission to strengthen cyber capacity and expertise globally by being a pragmatic, action-oriented and flexible platform for international cooperation. The unique structure of the GFCE as a bottom-up, neutral and apolitical forum provides an excellent opportunity for multistakeholders to exchange best practices and expertise on cyber capacity building.

Members and partners work together on cyber capacity building through Working Groups. The GFCE Working Groups are based on the five prioritized themes in the Delhi Communiqué, seeking to encourage multistakeholder dialogue on the implementation of cyber capacity building: bringing together needs, resources and expertise. The five themes are:

- Cybersecurity policy & strategy (A);
- Cyber incident management & critical information protection (B);
- Cybercrime (C);
- Cybersecurity culture & skills (D);
- Cybersecurity standards (E).

For more information about the GFCE and its Working Groups, please visit https://www.thegfce.org or get in touch with the GFCE Secretariat at contact@thegfce.org.

A short guide to stakeholder engagement for National Cybersecurity Strategy development

GFCE WG A - Task Force Strategy & Assessments

Introduction

Stakeholder engagement is key to the success of any project and is often more of an art than a science. Initial stakeholder consultations and core consultation events are crucial for different aspects of the National Cybersecurity Strategy (NCS) development: from building relationships and trust and confidence in the process to training and capacity building of stakeholder groups which have not been involved in cyber issues before, to the actual focus groups and round table discussions which are essential to gather the evidence, perspective, and input to the NCS.

The development and implementation of effective cybersecurity policies and strategies can help realise social and economic benefits. When developing cybersecurity policies and strategies, it's important to work towards a cyberspace where threats are tackled in an effective way, and individuals can exercise their rights and freedoms. The COVID-19 pandemic has both accelerated demand for digital services at a pace never seen before and increased the attack surface and impact for threat actors to exploit, adding to the complexity of this already delicate balancing act and bringing cybersecurity strategy into sharp focus. At a time when cybersecurity strategy is increasingly important, yet social distancing constrains our ability to meet in person, how do we continue to effectively engage remotely?

This short guide to stakeholder engagement explores: (1) Why stakeholder engagement is important; (2) How to involve stakeholders; (3) How to improve the experience of stakeholders when working remotely; and (4) key recommendations for international implementers.

The identified good practices consider the perspectives of governments, regional organisations, implementers, civil society organisation and academia. The advice has been informed by the discussions at a webinar organised by Global Partners Digital (GPD) and the Global Cyber Security Capacity Centre (GCSCC) in March 2021. Presenters included Daniela Schnidrig from GPD, Cynthia Wright from MITRE, Geraldine Mugumya from NITA-Uganda, Nthabiseng Pule from Cybersecurity Capacity Center for Southern Africa (C3SA), and Kerry-Ann Barret from the Organization of American States (OAS).[1]

The webinar was part of a series of online sessions organised by the GCSCC and its regional partners, the Cybersecurity Capacity Centre for Southern Africa (C3SA) and the Oceania Cyber Security Centre (OCSC) and was a contribution to the Global Forum for Cyber Expertise (GFCE) Task Force "Strategy & Assessments".

[1] GCSCC (2021): Stakeholder Engagement in Cyber Policy Webinar Recording, https://www.youtube.com/watch?v=_TmxYpJBels

Why stakeholder engagement is important

There are 7 key benefits to engaging stakeholders in cyber policymaking and, in particular, in the NCS process[2]:

1. **Understand the priorities:** engaging stakeholders will help to ensure that the policy is addressing the correct issues and tackles real problems. Stakeholders understand the challenges that the officials in government may not always be aware of.
2. **Gain additional expertise to improve policy:** consulting with experts from different stakeholder groups provides diverse input to improve policy (see GPD guide "better informed and evidence-based policy outcomes"[3]).
3. **Ensure ownership of the NCS:** actors are more likely to buy into the implementation of the NCS if they had a chance to contribute and were part of the process, even when not all their priorities are included**.**
4. **Build trust and credibility:** stakeholder involvement creates trust and gives credibility to the whole policy process.
5. **Deliver meaningful outcomes:** getting consensus with stakeholders in the NCS development and its implementation helps guide how they and governments invest (see GPD guide "more effective implementation"[4]).
6. **Demystify cybersecurity:** the engagement of different stakeholder groups contributes to creating awareness that cybersecurity is not just a technology problem, but a people and process problem which affects all parts of society.
7. **Support education & awareness:** There are many programs run by stakeholders outside government initiatives. The engagement processes can promote the understanding of who is doing what and how different stakeholders can collaborate to achieve greater impact. Also, there are groups that may be unaware of the cyber issues and why it is important; engagement and consultations increase cybersecurity awareness and strengthen capacity (e.g., CMM assessments[5]); through the process, stakeholders also learn from each other, what has worked and what is needed.

[2] To learn more about stakeholder engagement in NCS development and implementation, see GPD and OAS/CICTE (2022): National Cybersecurity Strategies: Lessons learned and reflections from the Americas and other regions, publication forthcoming, and GPD (2018): Multistakeholder Approaches to National Cybersecurity Strategy Development, https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/

[3] GPD (2018): Multistakeholder Approaches to National Cybersecurity Strategy Development, https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/

[4] Ibid.

[5] GCSCC (2021): CMM Review Process; https://gcscc.ox.ac.uk/cmm-review-process

How to involve stakeholders

Now that we have touched on the benefits of engaging stakeholders, how should you involve them? The following steps are a great place to start:

1. **Define who you understand are the relevant stakeholders for the NCS process** (see GPD and OAS/CICTE Guide[6] and CMM assessments stakeholder list[7]).
2. **Map and prioritise your stakeholders from the whole society view**: list and sort stakeholders that are critical in terms of interest and influence. Consider who has relevant expertise at the national level and if they can contribute to the national goals. Think of people working on policy, those with technical background and those who may not have been involved in NCS processes before. Break down the different civil society groups in subgroups based on skills and areas of expertise.
3. **Survey your stakeholders:** understand what their needs and interests are in terms of the NCS and assess what tools and resources they need to participate in the process meaningfully.
4. **Make sure that stakeholders understand why their involvement in the NCS process is important:** connect to the goals that people already have (e.g., economic security or political security).
5. **Create Ownership:** focus engagement early on to explain and make connections regarding what cyber can enable for the respective institution (e.g., ministry), the economy and the government. This will help policy makers see that they and their interests are represented.
6. **Ensure continuous engagement:** build a relationship and maintain it, engagement is not just necessary at the beginning and during the NCS development but also beyond (implementation phase). Communication is key!
7. **Define the level of engagement:** ensure clear communication on the level of engagement that you need with them in each phase (some need to be involved constantly, others may just need updates from you).
8. **Make sure to be inclusive:** support organisations which may have challenges participating physically or may need translation support (e.g., travel support, online consultation, translation services).
9. **Train & educate:** consider developing and delivering a training programme to stakeholders who are new to this NCS process. Build capacity of public servant helps to embed the skills in the administration as some of them will progress to key decision-making positions.
10. **Adapt the language to the different stakeholder groups to make the process more accessible**. Avoid language in the engagement that is too technical.
11. **Conduct consultations in different formats to maximise and leverage participation** e.g., face-to-face meetings, focus groups, roundtable discussions.

[6] GPD and OAS/CICTE (2022): National Cybersecurity Strategies: Lessons learned and reflections from the Americas and other regions, publication forthcoming

[7] Ibid.

12. **Facilitate networking and relationship-building among stakeholders.**
13. **Organise a kick-off event**: this can have the form of an official event with speeches by officials.
14. **Establish a national working group**: a multistakeholder working group can help liaise with their constituencies (with e.g., all regulators involved so those persons can help reaching to the entities).

How to improve the experience of stakeholders when working remotely

The following good practices are recommended for improving the experience of stakeholders when working remotely[8]:

1. **Internet connectivity is key**: reliable, secure, affordable, and extensive Internet connectivity is critical for success. Unreliable Internet access at any point can impact on the quality of interactions, with poor audio being a challenge to understand at the best of times but critical when communicating in different languages.
2. **Don't just talk**: displaying questions on screen can assist when communicating in different languages and give participants time to consider responses.
3. **Be mindful of the cost**: connectivity can be a significant challenge for participants located in a country where data is expensive. Often participants are joining from their personal network and paying for the data usage. Where appropriate, consider supporting the costs associated with participation to enable inclusion of diverse participants.
4. **Identify a local host partner:** where the engagement is external, identify a local host who can connect you with key stakeholders, navigate the local context and help coordinate meetings and encourage participation.
5. **Take time to build rapport and trust**: building rapport and trust remotely is more challenging yet critical to effective engagement. Take time to get to know a little about your stakeholders and what is going on in their lives, this is particularly valuable if you have never met before. Have virtual coffees with key stakeholders to get to know them. Enable chat functions so that participants feel comfortable with asking questions.
6. **Plan engagements in three stages to allow participants time to prepare**: first, meet and introduce the topic and explain why it is important, the benefit of participating, what is going to happen, how you will engage (survey, email, online meeting etc) and what participant need to do. Then send out resources several days ahead of the main engagement meeting to allow sufficient time for participants to read and ask questions. Finally, meet for the main engagement.
7. **Don't forget the user experience:** there are multiple platforms out there for remote engagement, all with their own quirks for installation and configuration. Different participants will have different preferences and in some cases are restricted to one

[8] C3SA, GCSCC, OCSC (2021): Reviewing cybersecurity capacity in a COVID-19 environment http://www.c3sa.uct.ac.za/c3sa/news/2020/review

option. Be flexible in your approach and use the platform that is best for your participants. Test and provide support to participants to ensure the best user experience prior to your main engagement.

8. **Video is important but be culturally aware:** when connectivity allows, video can help to build trust amongst stakeholders and enable facilitators to interpret facial expressions for feedback on how the engagement in progressing. However, in some cultures allowing participant to switch off the webcam will increase participation through an increased feeling of anonymity.
9. **Take time to map stakeholders:** one of the benefits of shifting to remote engagement is the increased accessibility for stakeholders who may not have been heard during face-to-face meetings due to logistical challenges or other reasons. Taking time to carefully identify and map stakeholders across the public sector, private sector and civil society can gain new and interesting perspectives that may have been missed before.
10. **Don’t forget the coffee and comfort breaks:** keep to an agenda you would use for face-to-face. Everyone needs a break. Ensure there are regular breaks to help participants feel refreshed and ready to continue. Break out rooms for virtual coffee breaks can be useful to shift the conversation and provide smaller groups time to talk, but the platforms typically require break outs to be facilitated and remember a breakout is not really a break.
11. **Use multiple methods to continue to engage with key stakeholders:** engagement doesn’t have to stop when you click ‘end meeting’. Provide key stakeholders with multiple methods of engaging with you and continue to engage. This can help not only when preparing for the main engagement and trouble shotting challenges but also ensuring desired outcomes.

Key recommendations for International Implementers:

1. **Build a relationship with a government interlocutor who is your coordinator/face in the country**. For the first contact go through the diplomatic channels, international partners or implementers who are already active in the country. If a government is not very functional or there are elections or a change of personnel, focus on identifying which members of society you can engage with (e.g., civic, churches or schools). Building capacity of public servant helps to embed the skills in the administration as some of them will progress to key decision-making positions.
2. **Define your role and responsibilities:** be clear and aware of your role: e.g., neutral interlocutor and facilitator who has the ability to convene and brief.
3. **Communicate actively and regularly:** encourage the government to stay involved, e.g., send regular email updates; if necessary daily, weekly, bi-weekly using phone, e-mail, WhatsApp, Teams, whatever works best to ensure that the engagement is constant. Follow up on ideas which were shared during the consultations.

4. **Support mapping of stakeholders:** provide guidance to help the host identify stakeholders and encourage them to invite key players from the private, public sectors and the civil society.
5. **Focus on the experience for the stakeholder:** engage a local resource to provide support and advice on engagement. Online meetings must be free and easy to use, considerate of time zones, well organised, interesting, and short. Consider supporting the costs associated with participation in enable inclusion of diverse participants.
6. **Ensure you take a flexible approach:** be prepared to adapt to your stakeholders requirements and remember no matter what we plan for, the unexpected happens, especially so during a global pandemic.