GLOBAL FORUM ON CYBER EXPERTISE

Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle

Last updated: 10 June 2021

Authors

This Catalog was developed in 2020 as part of the Work Plan of the Global Forum on Cyber Expertise (GFCE) Strategy & Assessments Task Force, under the leadership of Robert Collett (former TF co-Lead), Carolin Weisser Harris and Lea Kaspar. The Task Force would like to thank the following organizations for their comments or contributions: Africa Cybersecurity and Digital Rights Organization (ACDRO), Cybersecurity Capacity Centre for Southern Africa (C3SA), Cyber4Dev, CyberGreen, CYSIAM, DiploFoundation, Global Cyber Security Capacity Centre (GCSCC), George C. Marshall European Centre for Security Studies, Global Partners Digital, International Telecommunications Union (ITU), MITRE, Ministry of Justice and Public Security Norway, NRD Cybersecurity, Organization of American States (OAS), Oceania Cyber Security Centre, the United Kingdom Home Office and the GFCE Secretariat.

About the Catalog

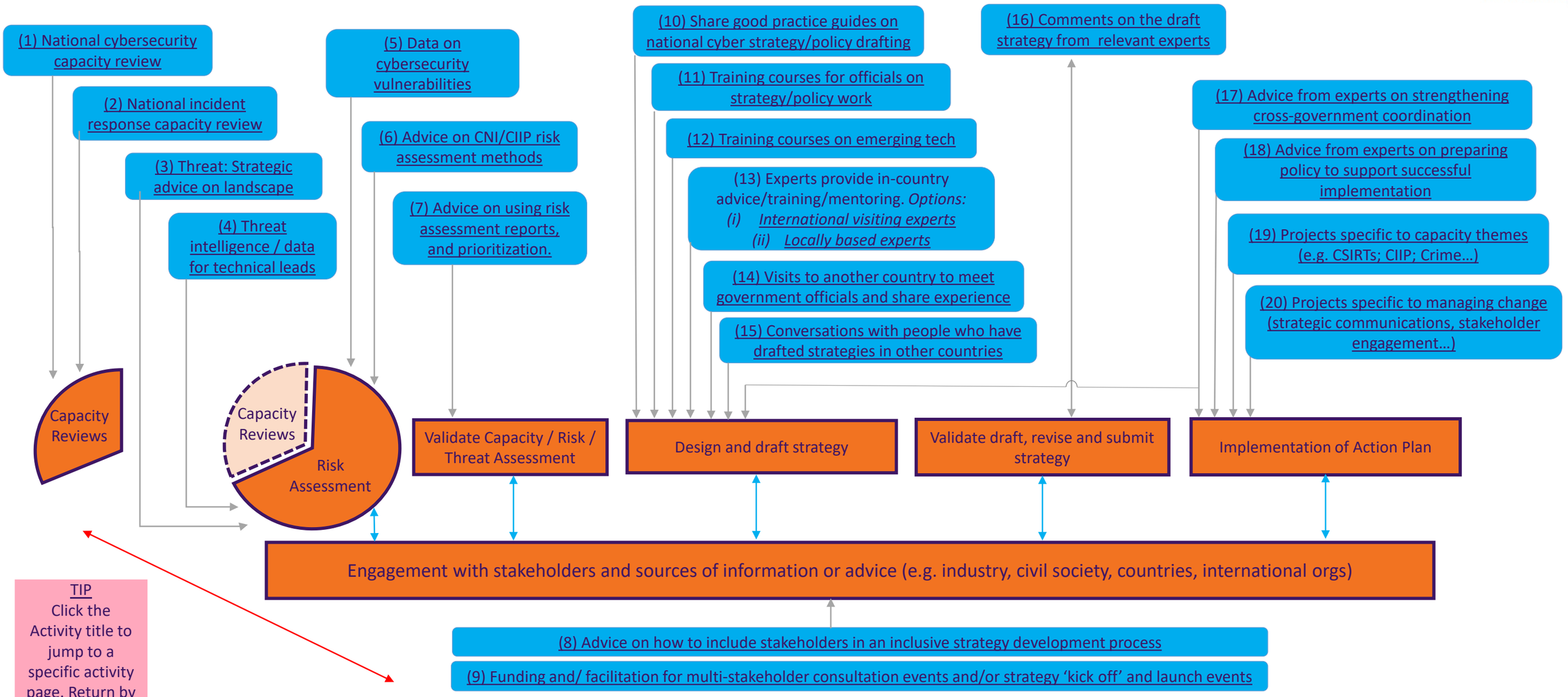
Objective

The objective of this Catalog is to inform countries of the types of support activities available from GFCE Members and Partners, and to help programme managers design projects. The Task Force aims to help countries requesting support for the National Cybersecurity Strategy (NCS) cycle by making the GFCE clearing house process more time efficient.

How to use

This Catalog offers examples of 20 activities that could go into a project supporting a country's NCS cycle. To jump to an activity page, click the title of the activity. To return to the home page, click the home icon on the top left of the activity page.

Types of activity that could go into a project supporting a country's cyber strategy cycle



TIP
Click the Activity title to jump to a specific activity page. Return by clicking the home icon.

Initiation | Stocktaking and Analysis | Production of the National Cyber Strategy | Implementation | Monitor & Evaluate

Good practice starting conditions for phases in the strategy cycle

(A1) Leadership interest

(B1) Lead official(s) support

(A2) Leadership support

(B2) Lead official(s) resourced to conduct analysis

(A3) Leadership instructs production phase

(B3) Lead official(s) resourced to produce strategy

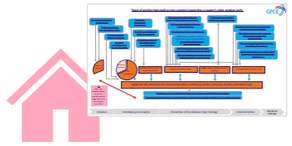
(C) Officials know what national goals/vision the strategy should support

(D) Stocktaking has identified critical functions/assets and assessed protective measures, national cyber capacity, threats and landscape.

(A4) Leadership commitment

(E) Budget processes to fund prioritized implementation.

Initiation → Stocktaking and Analysis → Production of the National Cyber Strategy → Implementation → Monitor & Evaluate



(1) National cyber security capacity review

ACTIVITY SUMMARY

What is the aim? The aim of a national cyber security capacity review is to help a country understand its current state of cybersecurity capacity at the national policy and capabilities level. A review is not a technical or operational study. It is also different from a comparative international survey, which typically results in a ranking table and not a report.

Why do it? You can only plan effectively if you know your current strengths and weaknesses. Furthermore, repeating a review every few years – for example at the start and end of a strategy – will help measure progress.

What are typical outputs? A report including maturity stages for various factors of cybersecurity capacity and recommendations for capacity-building activities and investment.

How is it delivered? Typically, international experts work with the government to run a few days of focus group workshops with clusters of people who understand the national cybersecurity landscape (e.g. policy makers; companies; police and judiciary; academics; civil society etc.). The experts then work with government officials to write and/or edit a review report, using the findings from the focus groups and desk research.

How easily can a country do it themselves? Some governments, especially more advanced ones, run the review process without international assistance using international models or their own design.

What good practice guidance is available? The GFCE's Cybil Portal has both a range of models that can be used, as well as links to published reviews: https://cybilportal.org/tools/?_sft_themes=assessments

TOP TIPS

- A country can conduct a review at any time, but there are a few popular options: before or during the initiation phase of a strategy to build interest; during the stocktaking and analysis phase to improve understanding; or during the monitoring and evaluation phase to measure progress.
- Many governments have chosen to publish their reports, because it helps to engage people in the national strategy process, it is an international confidence-building measure, and it helps to attract and coordinate international capacity building.
- Repeat the assessment after 3-5 years to track progress and to assess areas for further capacity building.

COST AND DURATION

Cost: The cost to a project is typically $65k - $130k USD depending upon the approach used. If funding is provided by a donor, the cost to the beneficiary country is almost zero: they often provide a venue for the workshops and handle invitations.

Duration: Once a government has formally agreed with the organization which conducts the review it takes about 6 months until the review is conducted and the report is submitted to the government.

CASE STUDY

In 2014, the Ministry for Economic Development of Kosovo, facilitated by the World Bank, asked the Global Cyber Security Capacity Centre (GCSCC) for assistance with a national capacity review based on the Centre's Cybersecurity Capacity Maturity Model for Nations (CMM) https://gcscc.web.ox.ac.uk/cmm-0. Through funding from several donors, the GCSCC was able to respond to this request, and prepared the CMM review process https://gcscc.ox.ac.uk/cmm-review-process.

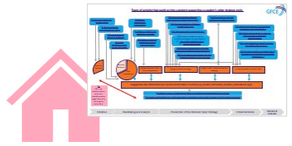
During February 2015, the GCSCC experts conducted ten focus group discussions over three days focusing on the five CMM dimensions: 1) Cybersecurity policy and strategy; 2) Cyber culture and society; 3) Cybersecurity education, training and skills; 4) Legal and regulatory frameworks; 5) Standards, organizations, and technologies. Each workshop brought together cybersecurity experts, such as critical infrastructure owners, policy makers, academia, civil society, representatives of the justice sector, as well as experts from the private sector.

Based on the information collected during the focus groups and follow-up desktop research to look for supporting evidence, the GCSCC drafted a report including recommendations for next steps that was reviewed by the subject matter experts the GCSCC for quality control before it was sent to the Kosovo government for feedback. After approval it was published on the ministry website.

Kosovo used the CMM review as part of their strategy planning process. Many of the recommendations in the review made it into official plans. Within a year of receiving the report the government had:

- Appointed a coordinating ministry for cybersecurity: Ministry of Internal Affairs.
- Run a multi-stakeholder strategy drafting process, using the capacity review as an input.
- Adopted its National Cybersecurity Strategy and Action Plan 2016-2019.
- Established a national CSIRT (KOS-CERT).
- Developed a concept document for critical information infrastructure and draft standards regulation. https://gcscc.ox.ac.uk/kosovo-what-followed-cmm-review

Four years later, in July 2019, the GCSCC returned to Kosovo for a CMM re-assessment. This was again facilitated by the World Bank as part of its Global Cybersecurity Capacity Program II https://cybilportal.org/projects/global-cybersecurity-capacity-program-ii/. The report provided insights on where the country had improved capacity since the first review but also identified areas for further capacity building and support in adapting current efforts to new developments:
https://gcscc.ox.ac.uk/files/cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf



(2) National incident response capacity review

ACTIVITY SUMMARY

What is the aim? To help the country assess the development needs for its national incident response capability at a deeper level than is provided by a national cyber capacity assessment.

Why do it? It is not essential to do this as part of the strategy process, but for a country with low national incident response capability it can be helpful to conduct this review while preparing for drafting the strategy, because one of the key questions for the strategy may be whether the country wants a national CSIRT and, if it does, which ministry or organization should be responsible for it.

What are typical outputs? A report on the current national incident response capabilities with recommendations for improvements.

How is it delivered? A small team of international experts will conduct one or two short visits to interview key decision makers, officials and other relevant stakeholders. They will then write a report.

How easily can a country do it themselves? The interviewing and report writing process could easily be conducted by a government team. The added value of using international experts is that they can provide advice during the process and in their report, based on experience working with many countries on setting up or strengthening national incident response capabilities. A report from an international organization may also help raise the profile of the issue locally. It may also avoid delays if there is no agreed lead ministry/organization to write the report.

What good practice guidance is available? GFCE WG B Lessons Learned on Cyber Incident Management Capacity Building. Three useful reference docs are mentioned in the Case Study (on the right). Others are available on the Cybil Portal.

TOP TIPS

- Experienced auditors must be involved for the best assessment outcomes.
- Focus should be on measurable results and outcome-driven approach, i.e. roadmap activities must be actionable and with defined measurable results
- Assessments must be paired with budgets and human resources available for the implementation of improvements.

COST AND DURATION

Cost: usually starts from $25k and up to $75k USD depending on scope and if travel is necessary.
Duration: Once a government has requested a review, there is normally one month to prepare for on-site consultations, one week to run the consultations and then one month for a report writing and finalization with the government.

CASE STUDY

In 2019, the Inter-American Development Bank (IDB) launched a project to support Ecuador's national cybersecurity policy formation as part of a wider aim of increasing policy makers' holistic understanding of cybersecurity in Latin America and the Caribbean. NRD Cyber Security was selected to implement this project and to support the formation of Ecuador's national cybersecurity policy by:

- Assessing the current situation, gaps and challenges in cybersecurity in Ecuador;
- Planning specific improvements to the government's cybersecurity readiness; and
- Supporting the National Cybersecurity Strategy formation process.

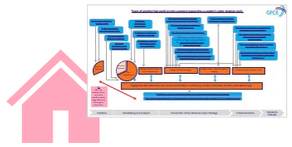
One of their first steps was to conduct a national incident response capacity review to provide tailored recommendations as to the direction in which Ecuador's incident response capacity should evolve.

Two NRD Cyber Security experts visited Quito and over four days held consultations with Ecuadorian public, private and academic incident response organizations. The aim of the consultations was to identify maturity gaps in handling cyber incidents Ecuador, the most relevant services needed to improve the security of government services, and what capabilities and technologies would ensure proper implementation of those services, and to assess whether the legal, organizational and operational environment would ensure proper enhancement of incident response capacities. The experts used three specific methodologies to identify cyber-incident response maturity and capability gaps:

- the SIM3 methodology was used to identify maturity gaps in terms of the national incident response team organization, staffing, tools and processes;
- the FIRST.Org Service Framework was used to help identify additional potential services that Ecuador's national incident response team should provide; and
- The SOC-CMM methodology was used to prioritize Ecuador's government incident response services and technologies needed to implement required services.

As a result of consultations, NRD Cyber Security experts drafted a report for the government of Ecuador with the assessment of the current cyber incident response capacities in Ecuador at national, governmental, sector and company level. They also provided recommendations for how government incident response capacity could be enhanced, building on capacities that they already have.

The cyber incident response capacity assessments and recommendations were integrated into the cybersecurity improvement plan for Ecuador. A separate roadmap for establishing a government Security Operations Centre (SOC) was prepared.



(3) Threat: Strategic advice on landscape

ACTIVITY SUMMARY

What is the aim? All countries are dependent on digital resilience for their economic prosperity. Providing strategic advice on the threat landscape allows countries to identify priority sectors and their threats in order to make risk-based decisions that are appropriate to their unique economic circumstances.

Why do it? Understanding in detail the particular impact of any damage or loss of capability arising from an attack or accident allows a country to focus on protection and resilience rather than just defense. Reviewing the threat landscape provides a generic overview of known and emerging threats. This is especially important for emerging economies where the impact of a national cyber incident could have a disproportionate impact on economic growth.

What are typical outputs?

1. Prioritizing critical services / organizations e.g. critical national infrastructure such as utilities and government networks and clearly defined roles and responsibilities for owning the associated risks
2. Identifying threat actors and their motivations unique to the country
3. Relationship of threat landscape to the national cyber strategy if one exists; if not, how it could be related.
4. Understanding of threat intelligence requirements

How is it delivered? Direct consultancy, facilitated workshops. Analysis of the major threats in relation to a prioritized list of national capabilities and organizations. Gap analysis compared to similar countries with a higher level of maturity.

How easily can a country do it themselves? Some external help will be needed to develop the foundation and set up the ongoing maintenance. Once a process has been established, awareness raised and priorities identified, then it is a relatively straightforward process.

What good practice guidance is available? The ENSIA (NCSC and all major security vendors) provide a regular report on the cyber threat landscape available here: https://etl.enisa.europa.eu/#/ - standard risk analysis frameworks help map this to specific vulnerabilities.

TOP TIPS

- The effectiveness of this activity is greatly improved by having a good understanding of what is critical CNI and CII, before providing strategic advice on the threat landscape. A series of workshops to develop this understanding is easy to implement and helps raise awareness.
- Having clearly defined roles and responsibilities within organizations that are accountable for security will steer the risk apportioned to each threat. Having this in place, as well as a good understanding of the national monitoring and detection capabilities, will also add value to the work. Again, these can be developed through workshops.

COST AND DURATION

Cost: $6,580 USD for facilitated workshops to develop understanding followed by $13,160 USD for a 1-year monthly mentoring and development service.

Duration: Circa 1 week for the initiation workshops followed by a 12-month light touch project to increase the national capability. Depending on how much support the country needs, this could be a little as one day a month mentoring or 4 days a month to deliver fully embedded and maintained capability.

CASE STUDY

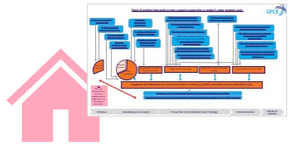
In 2019, CYSIAM were asked to work with an organization from a Middle Eastern country that had responsibility for the security of some public networks and had just suffered a serious cyber attack. CYSIAM's main effort was to help them recover from the attack, perform a post-incident analysis and assist with formally developing their appreciation of the threats unique to their country. They already had a good appreciation of the vulnerabilities of the organizations that they were responsible for; however, they had not formally carried out a threat landscape activity and so did not fully understand the strategic threat. The nature of the incident prompted the organization to bring in external and independent expertise to take a strategic approach to cybersecurity rather than focusing only on the technical controls.

CYSIAM initially focused on helping the organization understand the root cause of the recent incident and, using some analysis and threat intelligence, were able to relate it to an ongoing ransomware campaign. Once the immediate threat was identified, it was relatively easy to map across to existing and emerging threats to help network defenders and non-technical managers to understand the risks and build a remediation plan for this isolated incident. However, the organization recognized that a more proactive approach was needed.

As the organization clearly understood their priorities and existing vulnerabilities, CYSIAM carried out a series of threat landscape modelling workshops and used a number of sources to provide strategic advice on the current and emerging threats. These were principally the annual security reports from NCSC, the ENSIA ETL and the Mandiant Fire-Eye open-source analysis of existing, new and emerging threats. This threat-mapping activity allowed non-technical leaders in the organization to make prioritized decisions for current and future investment in preventative measures and allowed cyber defenders to shift their focus from response to resilience.

Because of the vulnerability analysis conducted on the organization, the support provided to the security team in learning from the incident and developing a mature understanding and effective prioritization of their responsibilities, CYSIAM were able to easily take threat data from and landscape analysis and apply the relevant parts to their organization. Most importantly, the organizations and staff involved were able to achieve a step change in their own capability by using a combination of vulnerability awareness, network prioritization and open-source cyber threat landscape data.

The next stage of maturity is to develop their own strategic threat landscape reporting once a good foundation has been established.



(4) Threat intelligence / data for technical leads

ACTIVITY SUMMARY

What is the aim? The aim of providing a threat intelligence and data for technical leads capability is to create a detailed technical awareness of relevant and sector-specific threats.
Why do it? It provides an immediate reference point for indicators of compromise and allows technical leads to understand if a particular threat has been seen before or is new and therefore requires a new approach. It is a critical part of incident response as being able to identify a threat / malware type quickly and accurately allows responders to understand what they are dealing with and eradicate it from a network.
What are typical outputs?

1. Routine monthly reporting detailing the generic threat landscape with technical data for defenders to use on intrusion-detection services.
2. A searchable repository of historic data for cybersecurity analysts to interrogate.
3. Tailored intelligence report based on the specific threat landscape of that country.
4. Immediate reporting by exception based on new or changing intrusion sets that pose a specific threat – for example if a new vulnerability is found then an exception-based report should be issued to raise awareness of this new threat.

How is it delivered? Normally as a service by threat intelligence specialists who provide access to an online portal and alerts via email for urgent reporting.
How easily can a country do it themselves? There are so many good products out there in open source, it is very easy to get started using threat intelligence however, it's much harder to produce propriety data and analysis.
What good practice guidance is available? CREST are the UK market leaders in threat intelligence best practice training but also the UK NCSC run a platform called CISP which provides threat intelligence and the opportunity for business and organizations to share data.

TOP TIPS

- Before a client purchases this capability from a vendor it is important to first map out the threat landscape relevant to the client. This means that the client requirement is mapped to a vendor's expertise. For example, some companies specialize in Russia, while others might focus on criminal gangs. However, they will all cover the same baseline of threats.
- Should the client wish to build their own capability then they need to focus on the diversity of skills required to take complicated subject matter and turn it into a report that a non-technical person can make a decision on. The UK NCSC assessment team are leaders in this, and their reporting can be found on the NCSC CiSP platform.
- The most effective solution is a blend of in-house expertise, professional reporting, and open source – making sure that relevant content is cherry picked to suit the threat landscape.

COST AND DURATION

Cost: subscription – free to $105,250 USD per year for big name vendors. For training an in-house team $6,580 USD of training per person + salary. However, a base level of technical knowledge is required.
Duration: subscriptions are normally yearly and to train someone from scratch requires about 3 months of training, mentoring and experience before they are effective - assuming a base level of technical understanding.

CASE STUDY

Scenario 1:

In 2018, CYSIAM were instructed by a UK-based organization to investigate the activity of a critical piece of infrastructure over a given time period in order to establish a baseline for future updates to their security plan. The organization had previously been susceptible to attacks and therefore also requested that we investigate likely threat actors for similar future attacks. We engaged with them to establish the scope, and began by gathering technical data of previous attacks, and Open Source Intelligence (OSINT) of attacks to similar organizations and infrastructure.

Through OSINT and, in particular, dark-web investigation of the likely threat actors, we discovered a wing of a well-known overseas group publishing instructions on how to carry out cyber attacks on similar organizations to our customer. This included PDF instruction manuals and videos promoting their group. The content of the website, videos and PDFs was translated into English and revealed several TTPs (Tactics, Techniques and Procedures) including tools used, victim type and the vulnerabilities they looked for when choosing the victim.

After analyzing the data that we had gathered, we suggested that the motivation for this campaign was anti-Western political activism with the aim that the attacks would remain deniable, due to the fact that they were publishing instruction manuals for other individuals. We immediately collated the relevant information in relation to this campaign into a brief intelligence report and delivered it to our customer, who was able to ensure that their critical infrastructure was hardened against these known vulnerabilities as soon as possible.

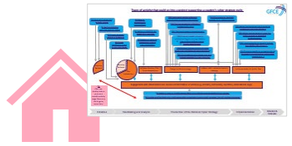
Scenario 2:

In 2019, we were asked by an Eastern European client to help develop their threat detection capability. They were starting from a very low level of maturity, consequently developing their own threat intelligence as per scenario 1 was too much of stretch. Instead, we helped them create a process for identifying sources of threat intelligence that were free and easy to access.

We used a combination of FireEye's Mandiant Advantage Free and the Malware Information Sharing Platform (MISP) to provide point and click reports on new threats. These platforms provide indicators of compromise and MISP provides an indicator-sharing function for partners who are also signed up to the service. This gave the client immediate access to threat intelligence.

Next, we advised on a development roadmap that would enable their own staff to be better equipped to perform their own analysis using research honey pots and other forms of data collection. We chose the CREST development roadmap for our students and supported them with ongoing mentoring.

This strategy enabled them to reach an immediate level of capability whilst developing in-house capacity in parallel. Within 3 months they were developing their own threat intelligence and sharing information with the international community.



(5) Data on cybersecurity vulnerabilities

ACTIVITY SUMMARY

What is the aim? The aim is to provide information that can inform the strategy and to help illustrate how evidence-based strategy making can work, using up-to-date cybersecurity data relevant to the country.

Why do it? Strategies are better when informed by evidence, especially timely and relevant data. However, policy makers may not have experience accessing cybersecurity data or using it to inform their recommendations.

What are typical outputs? A report on the health of the internet ecosystem in the country. See case study on the right.

How is it delivered? The consultant/organisation providing data and analysis will normally provide a document report and present the findings in person.

How easily can a country do it themselves? Countries can access the data themselves but may find it helpful to have a consultant/organisation identify good data sources for them and help them interpret the national data.

What good practice guidance is available? There is not a good practice document specifically on this activity.

Data sources countries might use include:

- CyberGreen – Provides statistics on vulnerabilities that cause DDOS risk (e.g. Open NTP; Open Recursive DNS)
- Mejiro – Is an online tool by JPCERT for visualizing national data on DDOS vulnerabilities.

COST AND DURATION

Cost: Internet Health Ecosystem analysis report: $20k – $30k USD/country (depending on risk indicators and depth of analysis).

Duration: 3 months.

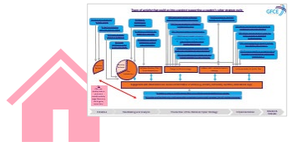
CASE STUDY

In 2019, the Economic Research Institute for South and East Asia (ERIA) asked CyberGreen to produce an Internet Ecosystem Health Analysis Report for ASEAN 10 countries. In 2018, World Bank Group asked CyberGreen to conduct Internet health analysis for East African countries at the East Africa Cyber Clinic.

CyberGreen collected data on vulnerabilities and risk conditions at the national level. They then conducted statistical analysis to assess the cleanliness of the Internet ecosystems within the countries and recommend specific policies and measures.

The Internet health risk indicators they used included:

- Systemic Vulnerabilities in the Internet Ecosystem: They uncovered open services which could be exploited as amplification DDoS attack infrastructure (Open DNS, NTP, SSDP, SNMP, CHARGEN). Raw counts of misconfigured devices were provided, along with trends over time, and breakdown by the top ISPs supplying or servicing those devices.
- Email Infrastructure Analysis: They assessed the level of implementation of the Sender Policy Framework (SPF) used for sending domain authentication, Domain Keys Identified Mail (DKIM), and DMARC (a technology for reinforcing SPF and DKIM domain authentication). This analysis tells the country whether these policies are being applied to avoid spam and other email-related threats.
- Other risk indicators, including:
    - Routing security performance
    - Ecosystem outdatedness
    - ISP security best practice implementation



(6) Advice on CNI/CIIP risk assessment methods

ACTIVITY SUMMARY

What is the aim? To help a country understand the national critical infrastructure and systems it needs to protect it at the moment and how strong its processes are for managing the risk to those assets.

Why do it? Countries should be able to identify and manage cybersecurity risks at a national level and use this to inform priority areas for future investment, which will be highlighted in a national strategy.

What are typical outputs? A list of critical national infrastructure and/or critical information infrastructure. And a report, produced by the government itself, on the risk mitigation measures for this CNI/CII and its adequacy.

How is it delivered? Typically, external consultants will bring together the government and private sector to establish a local team. They will train the local team, who will send questionnaires to the owners of CNI and together interpret the information that is sent back. The experts may help run a series of workshops to explain the process to stakeholders and, at the end, discuss the results.

How easily can a country do it themselves? Moderately easily. Example questionnaires and assessment methodologies can be requested from GFCE members. However, international experts will often have tools for analyzing the questionnaire data. They will also have expertise in interpreting the results.

What good practice guidance is available? The UK Home Office is developing a training portal and videos to enable remote delivery and to assist countries to train others.

TOP TIPS

- Spend time at the start talking to the owners of the CNI/CII to gain their trust in the process.
- Develop a local team of government and private sector representatives to encourage those who might be reluctant to participate.
- If a country is concerned about the confidentiality of the data, they can ask for the project to be designed in such a way that nobody other than the government sees the sensitive data and it is stored securely in the lead ministry.
- Build in time for the strategy process for the risk assessment, because it can take 6 months.

COST AND DURATION

Cost: Varied ($40k - $130k USD per country dependent on requirement to travel).

Duration: 3-6 months.

CASE STUDY

Sierra Leone National Cyber Risk Assessment (NCRA)

In 2019, the UK Home Office engaged with the Ministry of Information and Communications (MIC) in Sierra Leone as part of its Commonwealth Cyber Program. Sierra Leone had not undertaken a CNI cyber risk assessment before.

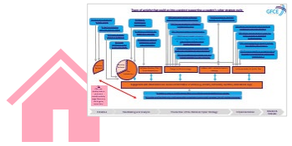
The local NCRA team (made up of both government and private sector representatives) brought together multiple key critical national infrastructure sectors to establish a baseline of risk to their critical information infrastructure. UK Government provided expert guidance and analytical training to build the capability within Sierra Leone. The UK team also supported the analysis of the results, enabling the local team to develop a list of key priorities for future investment.

This process took 5 months, from August 2019-January 2020, and MIC has committed to repeating the process periodically; Sierra Leone now has a national capability. A results report was developed with an agreed list of recommendations. The local team also committed to working with each sector/organization to share and further analyze the individual results in order to take forward the prioritized capability gaps.

From the UK team's perspective, the key outcome from the process was the improved relationship between the host government and their private sector. The activity was the catalyst required by the host Government to bring the various private sector stakeholders together for the first time. As a testament to bringing people together and the hard work by the local teams to build relationships, any initial distrust was transformed into strong relationships being built as the process went on. For example, a telecoms company reported a cyber attack to the government of Sierra Leone, which they openly admitted they would not have done prior to the NCRA process.

Training a hybrid team demonstrates the value of the NCRA and how it brings stakeholders together to build strong and trusted relationships; but it also showcases that cybersecurity is not just an issue for government. It is everyone's responsibility.

Within the 3-workshop NCRA approach, the UK team has embedded an immersive cyber exercise. We delivered the exercise with the assistance of the local team at the NCRA Results briefing with the sector stakeholders in order to highlight the dependencies between sectors and the importance of building resilience.



(7) Advice on using risk assessment reports, and prioritization.

ACTIVITY SUMMARY

What is the aim? To help countries use the information in their capacity and risk assessment reports, to guide the design and content of a national cyber strategy.

Why do it? In the Stock Taking and Analysis phase, countries should bring together evidence they collected, compare it and confirm it is valid. They should interpret that information, identifying key themes and issues that will inform the strategy. This is also a good point at which to set risk-tolerance levels.

What are typical outputs? An agreed set of evidence-based facts and assumptions that justify the identification and prioritization of critical sectors, processes and risks. E.g., "We assume economic expansion will remain a top national priority; vulnerabilities in the Financial Services sector represent the greatest cyber risk to this priority; and the greatest threat to the Financial Services is organized cybercrime targeting our national banks." A second output could be a baseline assessment of the effectiveness of current risk mitigation measures in priority areas.

How is it delivered? Workshops, facilitated discussions, and exercises.

How easily can a country do it themselves? Many countries can follow a process for validating risk reports and establishing priorities. External assistance can help: provide reassurance that things have not been missed; bring in external experience; break down departmental boundaries; and take a multi-stakeholder approach.

What good practice guidance is available? The best source is people who have done this before. See also, material in guides by: ENISA; OECD; GCSCC (CMM); and MITRE (NCSDI).

TOP TIPS

- Collect information and evidence from the very start (Activity 1).
- Facts and assumptions about the prioritization of risks and sectors should be communicated to senior government and political leaders; key industry representatives (especially from the prioritized critical sectors); and civil society organizations for review and concurrence.
- Consider digital risk priorities in the context of other national risks, which are fundamentally political decisions.
- In this phase and activity it is important to take a multi-stakeholder approach. Use it to get buy-in.
- Seek information and assistance from others who have done this before or in other countries.

COST AND DURATION

Duration: 1-3 months. Duration can be reduced if risk validation is conducted through periodic reviews during the development of the risk assessment.

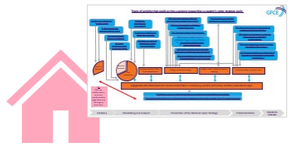
CASE STUDY

Several years ago, the MITRE Corporation assisted in the development of an African nation's national cyber strategy.

Assistance began with MITRE facilitating a comprehensive review of several key national capacity-building areas that are foundational to designing a national cyber strategy, including identifying key partnerships; the capacity to develop a cyber workforce; cyberspace governance mechanisms; and risk management approaches. These assessments helped identify the benefits that the country hoped to achieve through a cyber strategy, including socio-economic benefit and greater resiliency. Additionally, the country sought to build secure ICT infrastructure to attract more knowledge-based businesses to the country.

Risk management assessments were conducted with MITRE's assistance that involved identifying ICT threats and vulnerabilities that could impact strategic goals and objectives.

Findings from the risk assessments were included in the drafting of the strategy justifying the country's strategic approaches within government, as well as with the private sector and citizens. The development of this strategy included public, private, and academic stakeholders and established implementation governance that mandated a continuing public/private coordination body. MITRE also provided consultation on implementation priorities and methods. The commitment of public and private stakeholders and external assistance in limited, but key areas such as risk management, resulted in a comprehensive, feasible, and affordable national cyber strategy.



(8) Advice on how to involve stakeholders in NCSS development and implementation.

ACTIVITY SUMMARY

What is the aim? To support countries to involve relevant stakeholders in their national cybersecurity strategy (NCSS) development and implementation process in a holistic and sustained way.

Why do it? While there is an intrinsic value to involving a wide range of stakeholders in cybersecurity processes, there are two practical reasons why engaging stakeholders in the NCSS process specifically is beneficial:
1) involving stakeholders in policy development leads to better informed and evidence-based policy outcomes. Bringing stakeholders' diverse expertise into the NCSS process can help get a more accurate and evidence-based picture of the cybersecurity landscape, the possible implications of different policies being considered, and how best to engage with those other stakeholders during the NCSS's implementation and review stages; and
2) involving stakeholders in the development can lead to more effective NCSS implementation. Stakeholders who have been involved in the development of the NCSS will have a stronger understanding of the strategy and what is required from them, making implementation efforts more effective and sustainable, and it can also help build trust amongst stakeholders, which is crucial for smooth implementation.

What are typical outputs? A comprehensive NCSS development roadmap which includes a stakeholder map and stakeholder engagement plan.

How is it delivered? Through expert advice developed in close consultation with the policymakers via calls and/or in-person meetings.

How easily can a country do it themselves? Policymakers can draft the roadmap themselves using existing guidance documents.

What good practice guidance is available? GPD's "Involving stakeholders in national cybersecurity strategies: A guide for policymakers"

TOP TIPS

- Genuine commitment to inclusive approaches from governments is required (although not sufficient).
- Piecemeal approaches can only be partially successful; stakeholders should be involved throughout and in a holistic way.
- Reliance on local expertise can contribute to a roadmap that reflects local needs and context.

COST AND DURATION

Cost: Depends on the outputs and the format for delivery but would typically include staff time for the organization that is supporting the government in the process and hard costs for any related activities.

Duration: 3 to 6 months to develop a comprehensive roadmap that is informed by stakeholder input.

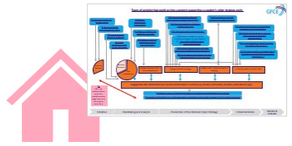
CASE STUDY

The OAS/CICTE Cybersecurity Program and GPD supported the government of Belize in developing their first NCSS. Belize's efforts to address cyber issues started in 2017, when the government organized the first National Cybersecurity Symposium, where the development of a strategy was identified as a key priority for Belize.

At the beginning of the process, an NCSS development roadmap was produced by the government with OAS/CICTE and GPD support. The roadmap included a holistic stakeholder engagement plan. Specific modalities for stakeholder engagement included:

- The establishment of a multi-stakeholder NCSS task force, set up under the leadership of the government's National Security Council Secretariat and tasked with drafting the strategy. It comprised 15 different entities, ranging from governmental stakeholders and the private sector to civil society and academia. The Task Force held around ten different meetings during the process.
- A capacity-building training, aimed at increasing awareness and building capacity of civil society actors to engage more effectively in the NCSS development process.
- Once a first draft was developed by the dedicated multi-stakeholder task force, an open online consultation was undertaken by the government with the aim of gathering 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 provide input.
- A multi-stakeholder workshop aimed at presenting the NCSS draft and gathering input and feedback from stakeholders, as well as to kick off discussions around implementation of the strategy.

OAS/CICTE provided the government of Belize with technical and strategy support to develop the NCSS with stakeholder engagement. GPD supported the process by developing and delivering a capacity-building program for civil society in Belize to increase their awareness and understanding of cyber policy issues and encourage their engagement in the NCSS development process. This process also demonstrated a mechanism where two implementers were able to use their resources complimentarily for the benefit of stakeholders and direct beneficiaries.



(9) Facilitation of multi-stakeholder events

ACTIVITY SUMMARY

What is the aim? To support efforts to gather stakeholder input to inform the different stages of NCSS development. The specific aim will depend on the stage of the process, but can typically include providing oversight, gathering information on the cyber landscape, proposing, reviewing or critiquing text, and reaching agreement on text, among other functions.

Why do it? There is an intrinsic value to involving a wide range of stakeholders in cybersecurity processes. In addition, there are two practical reasons why engaging stakeholders in the NCSS process specifically is beneficial: 1) involving stakeholders in policy development leads to better informed and evidence-based policy outcomes; and 2) involving stakeholders in the development can lead to more effective NCSS implementation.

What are typical outputs? Multi-stakeholder engagement efforts (e.g. consultations, workshops, kick-off and launch events)

How is it delivered? In-person or virtually.

How easily can a country do it themselves? Countries can do it themselves using available guidance or requesting assistance from experts on the topic.

What good practice guidance is available? GPD's "Involving stakeholders in national cybersecurity strategies: A guide for policymakers"

TOP TIPS

- The government should engage as wide a range of stakeholders as possible, so as to ensure that key perspectives and critical expertise are not missed. In the rapidly evolving digital environment, as new risks and opportunities emerge, the approach to identifying relevant stakeholders should aim to be as inclusive, flexible, and "future-proof" as possible.
- Depending on the existing interest and capacity of local stakeholders, additional investment and efforts might be necessary to build capacity and facilitate meaningful stakeholder engagement.
- Stakeholder input can be gathered virtually. Virtual events and online consultations may be particularly useful in cases where bringing people together physically poses practical challenges or costs are prohibitive.

COST AND DURATION

Cost: Will depend on duration, hard costs, the number of stakeholders involved, whether travel costs are being provided to participants or not, etc. Typically, an in-person consultation event can range anywhere from $1,770 - $12k USD (NB - this does not include additional capacity-building efforts; which would need to be budgeted separately).
Duration: A typical in-person event would last 1 to 2 days. An online consultation can last longer, depending on the overall process timeline.

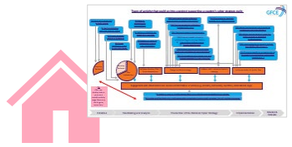
CASE STUDY

In March 2020, the Ministry of Information and Communication of Sierra Leone convened a **multi-stakeholder workshop**, as part of the government's efforts to develop the national cybersecurity strategy. The aim of the workshop was to increase awareness among stakeholders with regard to cyber policy issues, gather information on the landscape, increase coordination, and provide a space for stakeholders to discuss their priorities and inform the process of NCSS development. In addition to the stakeholder workshop, the Ministry co-convened a civil society training workshop in December 2019 to build the capacity of civil society groups to enable them to engage in cyber policy discussions, and the NCSS development process in particular.

In 2020, the Australian Government launched its new NCSS, the successor to its 2016 NCSS. As part of the strategy development, a series of **open forums** was convened in different cities across the country, as well as an initial **open online consultation,** which aimed to inform the strategy's development. The government published a cybersecurity strategy discussion paper and requested contributions from stakeholders. The paper outlined some guiding questions on specific cybersecurity topics, as well as a more open question for further consideration. The call for comments was open from September to November 2019 and gathered a total of 215 submissions. Public submissions were posted on the website of Australia's Home Affairs.

In Papua New Guinea, in 2017, the National Information and Communications Technology Authority invited stakeholders to provide written inputs via an **online questionnaire** to inform the development of Papua New Guinea's first national cybersecurity strategy.

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 the need for a detailed implementation framework, in order to help the NCSPS serve as a road map to address cyber threats. This final moment of assent from stakeholders was seen as essential to ensure broader community buy-in, and for 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 an open forum in October 2019 during Ghana's Cybersecurity Month, where the revised draft was presented for stakeholder input and validation.



(10) Share good practice guides on national cyber strategy/policy drafting

ACTIVITY SUMMARY

What is the aim? To help countries prepare their national strategies by making use of good practice guides that draw on experience from previous strategies and capacity building projects.

Why do it? It is a zero-cost way to share and encourage good practice.

What are typical outputs? The team drafting the strategy has access to global good practice and examples from other countries in the form of documents, meeting notes, website links and other media.

How is it delivered? In its simplest form, the team preparing the strategy can be sent links to good practice guides and databases with strategies, which can be found on the Cybil Portal. To go further, an implementer could sit down with the team to discuss the guides and how they could be drawn upon to inform the local strategy preparation process.

How easily can a country do it themselves? Very easily. They can access several tools and guidance documents on the Cybil Portal: https://cybilportal.org/tools/?_sft_themes=strategies and https://cybilportal.org/publications/?_sft_themes=strategies
Sometimes workshops are offered which help to use the good practice guides, e.g. by the ITU (see case study)

What good practice guidance is available?
Cybersecurity Strategies Evaluation Tool (ENISA, 2018)
Developing a National Strategy for Cybersecurity (Microsoft, 2013)
Good Practice Guide on National Cyber Security Strategies (ENISA, 2016)
Guide to Developing a National Cybersecurity Strategy (Commonwealth Cybercrime Initiative, CTO, Deloitte, GCSP, GCSCC, ITU, Microsoft, NATO CCDCOE, Potomac Institute for Policy Studies, World Bank, 2018)

TOP TIPS

- Look at different good practice guides.
- Have a look at existing NCS from the region or from countries with a similar set-up (size, GDP, culture, etc.).
- Read lessons learnt publications (e.g. "National Strategies – Interviews behind the cover. Senegal, Mexico, Norway, GFCE 2018 (see activity "*(15) Conversations with people who have drafted strategies in other countries").*

COST AND DURATION

Cost: Using the Good Practice Guide – Nil; workshops – mostly offered free of charge. However, participants may need to pay for their travel and lodging.

Duration: Using the Good Practice Guide – documents can be accessed immediately. Some time would be required for reading and for a discussion with implementers about the guides, if that was part of the activity. workshops – 1-3 days.

CASE STUDY

Using the Good Practice Guide: Kiribati drafted its NCS with support from the ITU using the *Guide to Developing a National Cybersecurity Strategy.*

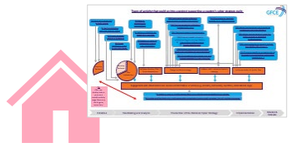
From 2019-20, the International Telecommunication Union (ITU) , in cooperation with member states and partners such as the Oceania Cyber Security Centre (OCSC) and Deloitte, also conducted four "Regional Capacity-Building Workshop on National Cybersecurity Strategy" workshops in Jakarta/Indonesia, Skopje/North Macedonia, Tunis/Tunisia and Melbourne/Australia which helped countries to utilize the good practice guide.

The workshops were targeted at participants from the respective region, such as ministry representatives, policy makers (parliamentarians), individuals in the judiciary system, regulatory bodies, national security agencies, military establishment (the units in charge of information security and/or IT and ICT management), law enforcement agencies, critical infrastructure providers (water, energy, transport, etc.), central monetary agency and banks, telcos and ISPs, and academia. National research bodies and local industry (private sector) involved in security initiatives could also benefit from the workshop.

The workshops built upon the *Guide to Developing a National Cybersecurity Strategy* and covered topics such as lifecycle of national cybersecurity strategy common principles on National Strategies (what it is, mission, vision, etc.), national cybersecurity strategies worldwide, approaches, comparative analysis, and the establishment of a governance structure to develop/maintain NCS. The training was completed with an exercise.

Sometimes these workshops were organized in the context of other events to ensure that as many interested individuals from the governments were able to participate and to make the best use of travel time and efforts. For instance, the Melbourne workshop was co-organized with the OCSC in the context of its Annual Conference and the GFCE Pacific regional meeting.

For further reading: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/NCS_Outcome_Report.pdf



(11) Training courses for officials on strategy/policy work

ACTIVITY SUMMARY

What is the aim? To enable countries to have an understanding of the nature and magnitude of today's global cybersecurity threats, and to develop a common understanding of the lexicon, best practices, and current cybersecurity initiatives within the public and private sectors. Countries also build networks of contacts with officials involved in cybersecurity strategy from other countries and regions and get connected with cybersecurity leaders from the public and private sectors.

Why do it? It is a very good way to gain comprehensive knowledge about cybersecurity policy on the global level and how it influences national strategies. Also, officials build a network with other government representatives and cybersecurity experts from other countries in their region and globally.

What are typical outputs? The participants gain the skills to provide leadership in the country on cybersecurity strategy and pursue a whole-of-government approach to cybersecurity.

How is it delivered? 2-3 days courses and workshops, regional summer schools, four-week residential course

How easily can a country do it themselves? The country has to get in contact with the training provider or reach out to the GFCE to find out who is offering training courses. In many cases the costs are covered (sometime travel costs have to be covered by the participant).

What good practice guidance is available?

- George C. Marshall European Center for Security: *Program on Cyber Security Studies (PCSS)*
- ITU Regional National Cybersecurity Strategy workshops (see Activity *10*)

TOP TIPS

- Ensure that as many people as possible in relevant positions participate in courses on a regular basis.
- Facilitate knowledge exchange after the completion of the course so the participant's home institution is also profiting.

COST AND DURATION

Cost: Depending on the program, courses are free of charge or travel and subsistence have to be covered by the participants.

Duration: A couple of days to several weeks.

CASE STUDY

Since 2014, the George C. Marshall European Center for Security Studies ("Marshall Centre") in Garmisch-Partenkirchen/Germany has been bringing together senior government officials from around the world for the *Program on Cyber Security Studies (PCSS)*. PCSS is strategy and policy-focused, non-technical and designed for cyber professionals who need to make informed decisions pertaining to cybersecurity strategy and policy. The residential course is 2.5-weeks long (13 contact days) and takes place each December.

The aims of the PCSS are to address the many challenges in the cyber environment while adhering to the fundamental values of democratic society. The program helps participants appreciate the nature and magnitude of today's threats, and develops a common understanding of the lexicon, best practices, and current initiatives within the public and private sectors. The curriculum emphasizes non-technical strategic solutions for enhancing cybersecurity. Course objectives cover techniques, policies, and best practices used to secure and defend the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems residing in the cyber domain.

PCSS provides participants with transnational cyber skills and prepares individuals for positions as senior-level cybersecurity leaders throughout government, and focuses on whole-of-government approaches to promote:

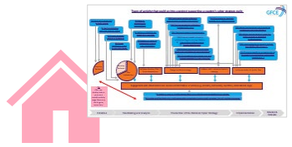
- Strategy and policy development
- Cyber aspects of critical infrastructure protection
- The role of the private sector in information and cyber technology
- Detecting and combating cyber crime
- Global collaboration and information sharing
- Understanding the transnational cyber environment, including national approaches in the United States, Germany, the European Union, NATO and other International organizations.
- Cyber policies in countering terrorism
- Identifying measures for cooperation on detecting and mitigating cyber incidents.

The program is tailored for senior officials responsible for developing or influencing cyber legislation, policies, or practices. Participation is open only to serving government officials and is ideal for diplomats, legislators, ministerial staff, policymakers, military and law enforcement officers, and other officials who require a better appreciation of cybersecurity.

The program is taught by world leaders in cybersecurity and allows participants to network and establish contacts with other cyber-focused professionals from every region of the world.

In addition to the residential course, the Marshall Centre organizes a number regional events throughout the year.

For more info: https://www.marshallcenter.org/en/academics/college-courses/program-cyber-security-studies-pcss



(12) Training courses on emerging tech

ACTIVITY SUMMARY

What is the aim?
To improve the individual and institutional capacity of policymakers and other officials in understanding the basics of emerging tech and the policy aspects related to the development of new technologies
Why do it?
Policymakers and other experts need to have a basic understanding of the new technologies, and the policy implications from a multidisciplinary perspective (including security, economic, development, and legal issues). It is by considering the various angles that policymakers can make informed decisions.
What are typical outputs?
Improved understanding and capacity, and the ability to ask the right questions when it comes to how technology is being developed. Ultimately, this leads to stronger institutional capacity.
How is it delivered?
Many courses can be taken virtually. The value-added of online training is the opportunity to interact and learn from participants from other countries or regions.
How easily can a country do it themselves?
Governments can consider tailor-made training based on their institutional needs or can support the participation of officials in taking existing courses.
What good practice guidance is available?
- *Reviewing Global Internet Governance Capacity Development and Identifying Opportunities for Collaboration*, Prepared for ITU by DiploFoundation, April 2017
- *Assessment of the Internet capacity development needs of IGF stakeholders*, Prepared for the IGF by A. Esterhuysen, February 2020

TOP TIPS

- In order for officials to gain the most benefit from online training, they need to be encouraged and supported by their institution to allocate the time required for their training, as part of their work.
- Capacity building is also more effective if it a part of an institution's policy for furthering the education of its officials.
- In order for the training recipients to continue benefiting from the knowledge generated during the training, it is recommended that the training resources and materials remain accessible for the participants indefinitely.
- Online or blended learning combine the possibility of advancing one's knowledge, with the flexibility that online courses offer in terms of schedules.
- Self-paced courses are a good option for participants who need maximum flexibility; however, lecturer-based courses ensure better course completion rates.

COST AND DURATION

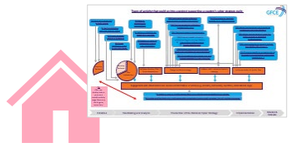
Cost: The cost of a training program depends on the course chosen.
Duration: Most online courses are between 4 and 8 weeks in duration. Training (and duration) can also be tailored to the organization's needs.

CASE STUDY

DiploFoundation is one of the leading global organizations providing capacity development in digital policy to policymakers, diplomats, and other practitioners. Diplo courses are well known for their asynchronous and lecturer-led methodology, and for the hypertext system of annotations, which enables participants to build discussions directly on the lecture texts. Diplo has been providing online training since 2002.

In 2019, Diplo launched the course on *Artificial Intelligence: Technology, Governance, and Policy Frameworks* in response to the growing demand for capacity development on various aspects of AI. The course builds on Diplo's own ongoing research in the area, and covers terminology, historical and philosophical background, technological basics, key players and forums, governance and regulation of AI, socio-economic aspects of AI, AI and security (including cybersecurity and lethal autonomous weapons systems), and AI and human rights. The course offers a broad overview of social, economic, human rights, and ethical implications of AI with a focus on the needs of diplomats, policymakers, and other interested audiences. It discusses the policy implications and the debates within various international organizations and between countries. It also touches on important topics related to competition and cooperation between countries and regional and global AI governance.

Three other long-standing courses offered by Diplo with a focus on emerging tech are:
- *An Introduction to Internet Governance*, which looks at technological developments from interdisciplinary angles;
- *Internet Technology and Policy*, which includes dedicated sections on emerging tech including big data, blockchain, IoT, and augmented and virtual reality;
- *Cybersecurity*, which also covers the security and cyber-diplomacy implications of the emerging tech, such as AI and lethal autonomous weapons, IoT and smart environment, virtual reality and 3D printing, as well as protocols like QUIC, DNS over HTTP and TLS, or Delay/disruption tolerant networking.



(13) Experts provide in-country advice/training/mentoring

ACTIVITY SUMMARY

What is the aim? To improve the capacity of officials and decision makers in the partner government to strategically plan and oversee the implementation of their strategy.

Why do it? Experts have experience to share from the strategy process in multiple countries and will often also have competence in training, coaching and running workshops. In-country, in-person capacity building is the common way for experts to provide their support within a project.

What are typical outputs? There can be a wide range of outputs, but often include increased capacity of those being trained, advised or mentored. For example, officials and decision makers have gained knowledge of the critical issues in drafting and implementing the strategy and understand what the necessary processes are.

How is it delivered? Many options including discussion meetings, training sessions and workshops. They can also embed within the drafting team and use a desk in their office, some or all of the time.

How easily can a country do it themselves? A country could contract directly with experts. Several implementers provide similar services under direct contract to governments and via capacity-building projects.

What good practice guidance is available? What good practice guidance is applicable will depend upon the topic the international experts are building capacity to address. Strategy guidance docs are listed at Activity 10. RAND Europe wrote their "Developing Cybersecurity Capacity. A proof-of-concept implementation guide" as a guide that could help officials or project experts as an aide memoire for good practice resources across all themes of capacity building.

TOP TIPS

- Whether the experts are flying in or locally based can change a project in several ways: timing; flexibility; how they deliver their support; budget; local perception, etc. This is explored in more detail on the next page.
- When using experts, be clear whether they are meant to provide capacity building, capacity augmentation or capacity substitution, and monitor whether the reality matches the plan. There has traditionally been a pressure on experts to draft strategies rather than use strategies.
- Discuss with the drafting team and the expert(s) where the final strategy will be on the continuum from a standard template (or another country's strategy) at one end to a completely unique structure at the other.

COST AND DURATION

Cost: The costs normally comprise a daily rate, expenses, travel, accommodation (if visiting) and security. The cost range is very wide, reflecting the range of complexity and duration from a single workshop to multi-year, locally based teams.

Duration: Experts may be needed for only a one -day workshop. However, if supporting the Stocktaking and Production phases of strategic planning, the duration could be anywhere up to a couple of years.

CASE STUDY

For several years, MITRE has been supporting the development and implementation of an African nation's cyber strategy.

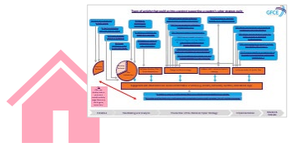
MITRE's expert consultation was first employed during an in-country engagement designed to assess the country's capacity to develop and implement a cyber strategy. This engagement included a facilitated discussion on identifying the country's national aspirations and the need for secure ICT infrastructure to achieve those aspirations. This facilitation involved high-level government and industry leaders and resulted in comprehensive recommendations regarding next steps for the host country as well as for other government donors.

Follow-on work included a comprehensive in-country risk management workshop that included public (including law enforcement, military and regulatory agencies) and private stakeholders who collaborated in defining national threats and vulnerabilities, as well as risk mitigation approaches and priorities.

Additionally, MITRE provided expert consultation remotely by reviewing important strategic documents. The key to expert engagement in these efforts was including comprehensive 'next step' recommendations in expert reports and assessments that provided the host country with options for timely and pertinent expert involvement, including the potential for provisioning technical expertise for sector-specific risk assessments and mitigation determinations; expert program and "change" management support; national cybersecurity awareness program development; and incident response and recovery organizations and exercises.

More Top Tips:

- Planning well-timed expert interventions can help a country maintain implementation momentum.
- Align the experience of experts used to the priority implementation needs of the country.
- Clearly identify the roles of experts regarding whether they are meant to provide capacity building, capacity augmentation or capacity substitution, or track implementation and make recommended modifications. When an expert drafts a country's strategy and implementation plans for them, this is not capacity building; it is capacity substitution.



(13 Continued). International vs. Local experts.

NATIONALITY OF EXPERTS AND WHERE THEY ARE BASED: WHY IT MATTERS

Feedback on past projects and lessons from the development community suggest that the nationality of experts and where they are based is an important issue for capacity building. Until now cyber capacity building projects have mostly deployed international experts on short visits. This was influenced by, among other things, the shortage of cybersecurity experts, especially in developing countries, and the low appetite for taking risk. However we are beginning to see three trends that may change this:

- there is more interest in contracting local implementing organizations and consultants, who have the nationality of the beneficiary country and are locally based;
- some projects are deploying international experts to be locally based for 6+ months at a time, or they are recruiting in-country international expat experts who happen to live locally already; and
- more projects are using regional international experts, who can visit more easily and frequently than those coming from farther afield.

Each type of expert has its own advantages and disadvantages. Using visiting experts can allow for more flexibility to change project direction and opens up a wider pool of experts to draw from. Locally-based experts can be more flexible in how and when they provide their assistance, and more easily follow up training and workshop sessions with monitoring and further support. In some contexts, an international expert may be listened to more closely than a local national, while in others the local national, or someone from the region, may receive greater attention. Individual skills and experience of course play a large role too.

In a number of GFCE meetings, governments have said that they would prefer that projects strengthened the pool of local experts so that they could be self-reliant in the future. However they have also asked funders and implementers to be careful when doing this and consider the secondary consequences of hiring local experts for projects. Projects can attract essential staff away from government and/or create unintended divisions within the local cyber community as some benefit from well-paid project assignments and others do not. This can be particularly acute where projects pay top-up salaries to officials or hire officials who are working for a project in addition to their government day job.

ADVICE FOR USING INTERNATIONAL EXPERTS

- International experts who are not locally based can strengthen their relationships and understanding of the local context by connecting together a series of visits and staying in touch remotely. This can have more impact than ‘fly in and fly out’ for a one-off training.
- International experts can form partnerships with a local expert and work as a team. Expertise can be transferred within these teams in both directions.
- Project beneficiaries can be involved in the selection of international experts.
- Consider using an international expert from the region (e.g. from a neighboring country).
- Consider providing international experts with training or briefings on the local political, cultural and digital context before they deliver activities.

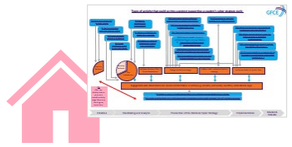
ADVICE FOR LOCALLY-BASING INTERNATIONAL EXPERTS

- Make use of experts you already have in your international networks (e.g. some countries have networks of law enforcement officers who could take on cybersecurity capacity building responsibilities)
- Locally based international experts are commonly used in international development programs.

ADVICE FOR USING LOCAL NATIONAL EXPERTS

- Design team management processes that include and make use of your local national experts. This may have been made easier because of the ‘remote working by default’ team management approaches developed for COVID19.
- Consider how you can provide support and skills transfer to your local national experts.
- Mitigate the risks of income differences between government employees and local (or international) consultants and staff with topped up salaries.

.



(14) Visits to another country to meet government officials and share experience

ACTIVITY SUMMARY

What is the aim?
The aim is to transfer knowledge between countries about how institutions, policies and context influence the development of national cyber security capacity. The host country will share lessons learned with a view to avoiding similar mistakes being made and to augment the beneficiary planning around capacity priorities.

Why do it?
To share institutional and strategic lessons on the development of a country's national cyber security capacity.

What are typical outputs?
The team responsible for developing national cyber security capacity institutions is challenged to consider how the lessons shared by the host government are relevant to its own capacity.

How is it delivered?
The host government provides access to cyber security and associated institutions within their government and, where relevant, industry sectors to provide a broad understanding of the institutional complexity of the host's cyber security framework.

How easily can a country do it themselves?
A country could request bilateral engagement with a host government, but this would place the financial burden on the two governments and may lead to a more political rather than working-level engagement.

What good practice guidance is available?
Some governments publish the details of their institutions, frameworks and strategies, but these rarely provide a clear understanding of how the different functions were developed and operate.

TOP TIPS

- Timing and need are key to this form of engagement. To be of most benefit to the beneficiary, such an engagement will take place before the implementation of a national strategy, in advance of the setting up of - or proposed changes to - the cyber security institutions and framework of the country.
- It is vital that the right beneficiaries attend the engagement. Particularly those with decision-making authority in order to apply the lessons learned effectively.
- Consider program funding restrictions when considering the wider engagement as the host government may wish to coordinate its own social or cultural functions outside of the capacity-building activities.

COST AND DURATION

Cost: Travel and subsistence costs for beneficiary attendees, possible costs for venue if host government does not use own premises.
Duration: Multiple days of engagements 2-5 days depending on the number of host government departments visited. Plus the planning and preparation time.

CASE STUDY

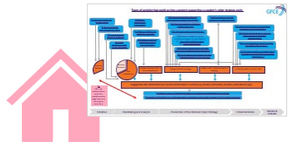
Sri Lanka was a phase 1 beneficiary country of EU Cyber Resilience for Development. They had just commenced implementation planning for the delivery of their first national cybersecurity strategy when the program initially engaged. Beneficiaries were keen to learn from the experience of European countries that had more recently gone through the same institutional journey. In particular those which had been willing to consider whole-of-government structures as part of the delivery of the first national cybersecurity strategy.

The study visit concept arose in meetings with the Sri Lankan Minister for Information Technology and Digital Infrastructure, the program delivery team and EU officials. The Minister felt that it would be of value to engage at a strategic level with a country of similar size which had recent lessons to share about cybersecurity capacity development. The program team and EU Officials worked with the government of Portugal to assess the viability and logistics of such an engagement.

The Sri Lankan Minister responsible for the cyber portfolio, accompanied by senior cybersecurity, legal and wider government officials, travelled to Portugal for 5 days including travel time. The Cyber4Dev team deployed supporting experts with experience of direct engagement with Sri Lanka, to provide neutral institutional and programmatic context in addition to translation and logistics support from the UK government. The delegation met with a wide range of Portuguese government departments from ministerial to working level, to share the full spectrum of lessons from their journey of capacity building. Structured engagements set across multiple days enabled the sessions to be host-led initially and then interactive latterly, based on what beneficiaries learnt and the questions which arose. Meeting with such a spectrum of officials in the host meant that peer relationships were formed for continuity of engagement.

Presence of program staff meant the capacity-building team was able to identify, validate and then support follow on activities which arose from the study visit. These ranged from a technical focus on certain solutions, to wider strategic considerations around the proposed structure of Sri Lanka's new cyber security agency.

Study visits which provide a whole-of-government perspective on cybersecurity capacity are valuable to countries which are early on in their journey. Such engagements aid the understanding of why a country has its particular cybersecurity framework of institutions. This assists beneficiaries in exploring different models and avoiding adopting a model which may not be the right fit in their national context..
Cyber4Dev has made use of other such visits by bringing together groups of beneficiaries to the countries which support the program. For instance, the government of Estonia has hosted working-level delegations to its cybersecurity agencies in order to showcase Estonian cyber capacity and to share lessons learned.



(15) Conversations with people who have drafted strategies in other countries

ACTIVITY SUMMARY

What is the aim? To build the capacity of the strategy preparation team by sharing knowledge and experience from people who have drafted national cyber strategies previously.

Why do it? This gives the team drafting the strategy direct access to the experience of people who have been in their position before. It can also create an international network of cyber policy influencers that they can draw on after the project.

What are typical outputs? The strategy team gains a network of contacts they can get advice from and exchange experience with.

How is it delivered? The project implementers can introduce the strategy preparation team to people who have drafted strategies in other countries. They can then stay part of the conversation or leave the drafting team to take forward the conversation.

How easily can a country do it themselves? Very easily. The GFCE is able to provide some introductions.

What good practice guidance is available? None specific to this activity.

TOP TIPS

- Reach out to the GFCE and its community. As many members have already drafted their own strategies or helped countries to draft strategies, they can share their experiences. As the GFCE has regular physical meetings, there are also opportunities to have those conversations in person.
- Acknowledge that every country is different and so is the drafting process and the NCS itself. Therefore, if you have conversations with several stakeholders, you can develop an understanding of what works and what doesn't in your country.

COST AND DURATION

Cost: Minimal.

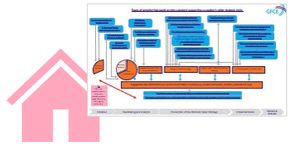
Duration: The conversations may take up to a month to arrange and then hold.

CASE STUDY

At the 2019 GFCE Annual Meeting in Addis Ababa, the GFCE's Task Force Strategy & Policy held a workshop for countries in Africa, at the end of which government delegates could sign up for a follow-on conversation with someone who had drafted a national strategy before. To prepare for the event, the task force asked for volunteers from its membership who had national cyber strategy drafting experience. It had already identified some volunteers from its earlier work to publish a booklet containing interviews with such officials from Norway, Mexico and Senegal.

During the NCS ITU workshops (see activity *10*), representatives from the government of North Macedonia shared experiences with participants from countries in the region.

One of the lessons from this experience was that people who have drafted a national strategy will often know others with the same experience, because they consulted internationally themselves while drafting. An informal network of strategy drafters is already forming. This is something that the GFCE and capacity building could make use of and support. However, it should remain sensitive to the fact that these policy officials will likely remain busy people and may not be available for more than a phone call.



(16) Comments on the draft strategy from relevant experts

ACTIVITY SUMMARY

What is the aim? To provide the strategy drafting team with feedback on their draft.

Why do it? Seeking feedback from people who have drafted a national strategy before provides an additional source of advice. Asking another country's strategy team to assist is a confidence-building measure and can strengthen a bilateral relationship.

What are typical outputs? The drafting team will receive comments and suggestions on the draft strategy.

How is it delivered? The drafting team request feedback from people who have previously drafted a strategy and/or bilateral partners.

How easily can a country do it themselves? Very easily. Countries will have bilateral partners they can request feedback from. Implementers and/or the GFCE can provide introductions to others who have drafted strategies.

What good practice guidance is available? N/a

TOP TIPS

- Reach out to your existing partners and stakeholders to ask for feedback.
- Get in contact with the GFCE which can introduce you to experts who can comment on the strategy.
- Consider publishing the draft document and inviting stakeholders to comment. This opens an additional opportunity for valuable input.

COST AND DURATION

Cost: Nil.

Duration: Allow a couple of weeks for finding experts who will help and then a couple of weeks will be needed for them to read the draft text and return comments.

CASE STUDY

Countries often consult partners, other stakeholders or the general public on their draft strategy which has become good practice:

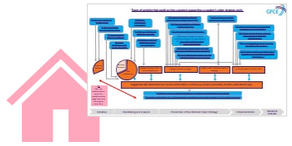
Botswana had already received assistance from, among others, MITRE and the Commonwealth Telecommunications Organization in preparing a draft. They then asked at least two bilateral partner countries, who were GFCE members, for feedback on the draft text.

Cyber policy officials in these two countries drew on their knowledge of their own national strategies and others in Africa to provide suggestions. As a result, the policy drafting team in Botswana were able to draw on advice from a number of sources and decide which feedback it felt was most appropriate to its circumstances and goals.

In 2018, the government of North Macedonia developed a national cyber strategy with assistance from the World Bank and after a CMM review by the Global Cyber Security Centre (GCSCC), they asked several partners, including the GCSCC, for comments on the draft strategy.

A broader consultation was chosen in 2020 by The Gambia, which published the draft documents of the National Cybersecurity Policy and Strategy, the National Cybersecurity Action Plans, the National Broadband Policy, and National Broadband Strategy on the Ministry's website and invited the public to comment. Additionally, the government asked the GFCE "Friends of The Gambia"* for feedback as part of the clearing house process.

*When a Clearing House request is underway, a "Friends of (requesting country)" Group is formed to coordinate existing projects, understand the detail of the requirement and provide advice when solicited.



(17) Advice from experts on strengthening cross-government coordination

ACTIVITY SUMMARY

What is the aim? To strengthen the capacity of the government to co-ordinate across its ministries, and with external partners and stakeholders, a process for overseeing the implementation of the strategy and action plan.

Why do it? A critical part of the strategic planning process is a cross-government process to coordinate and oversee the implementation of the new strategy and action plan. There is a greater likelihood of the strategy being used if the project helps the government prepare for this and start the process.

What are typical outputs? One size does not fit all, but a typical output would be a cross-government committee, with Terms of Reference and processes for its work.

How is it delivered? This activity is typically provided through advice and coaching. It may also involve exercises that demonstrate the importance of coordination and practice committee meetings.

How easily can a country do it themselves? Much of the work to prepare for and conduct the coordination is done by the government, applying their own experience and standard approach. They can ask other countries for their coordination lessons. An added value of the external experts, which can be hard to replicate internally, is that they provide a challenge function to question and test the coordination plans.

TOP TIPS

- Have a clear point of responsibility for coordinating and overseeing the implementation of the strategy.
- Make all stakeholders across government accountable and responsible for the follow up.
- Make the strategy relevant and known also for private sector and other external stakeholders, to increase the likelihood of a broad contribution on the follow up of the strategy.

COST AND DURATION

Cost: Dependent upon expert day rates, duration and whether you include exercises.

Duration: It can begin at the Strategy Production stage, or even earlier, and continue into the Implementation phase.

CASE STUDY

In Norway, the individual ministry is responsible for civil protection and emergency preparedness, including cybersecurity in their own sector. This implies responsibility for work on prevention, emergency preparedness and crisis management. The Ministry of Justice and Public Security (MoJ) has a general coordinating role in the area of civil protection and emergency preparedness, including cybersecurity across the whole of civilian society.

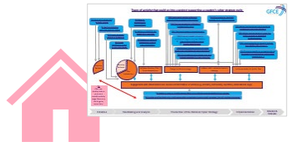
MoJ and the Ministry of Defense (MoD) were jointly responsible for drafting Norway's 4th national cybersecurity strategy. This ensured that the strategy covered the whole of government, both civilian and military aspects of cybersecurity, including the international dimension. The need for coordination was therefore large. A key for success was aligning the different stakeholders, making the strategy relevant and creating a joint feeling of ownership.

In the strategy itself, the Prime Minister had the foreword and also opened the launch conference of the strategy to show that the strategy is overreaching and a key priority. The opening also included contributions from the Minister of Public Security, Minister of Justice and Immigration, Minister of Defense and Minister of Research and Higher Education, together playing a vital part in presenting the different parts of the strategy. This showed that the challenges we face are cross-sectoral and a key priority for the whole government.

After the release of the strategy, all ministries received notifications from the MoJ about the expectations for follow up in all sectors. They were at the same time informed that they would need to report on the follow up to the MoJ and MoD about two years after the launch. This was seen as important to ensure focus on the follow up at an early stage and make different stakeholders accountable. As a part of the reporting on the follow up, the MoJ and MoD will conduct a digital questionnaire that will target both public and private companies across Norway. The questionnaire will measure the follow-up on the ten measures recommended as a part of the strategy to improve companies' own ability to prevent and handle cybersecurity incidents.

Both a public-private partnership forum and an inter-ministerial network have been established in Norway. These high-level groups are led by the MoJ and were consulted during the development of the strategy and to report on the overseeing of the implementation of the strategy.

Together, these activities and chosen approach have strengthened the coordination across government and external stakeholders, and at the same time increased the likelihood of successful implementation of the national strategy. In addition, it secured top level support and sent strong signals across society of the importance of the work on cybersecurity and the follow-up from the strategy.



(18) Advice from experts on preparing policy to support successful implementation

ACTIVITY SUMMARY

What is the aim? Technical assistance to strengthen the cybersecurity capacities.

Why do it? A national strategy is a broad and high-level document. Often countries will need to develop policies under the strategy to further define the government's position and what it will do. Policies might cover: the purpose and governance of the national CSIRT or National Cyber Security Centre (NCSC); cyber skills and education; cyber standards for industry and government procurement; international engagement.

What are typical outputs? Manuals, training and workshops.

How is it delivered? Online through different methodologies: reports, virtual meetings, online cyber exercises, organization of cyber woman challenges.

How easily can a country do it themselves? Not very likely as often the capacities may not be resident in country; support and expertise from international organizations is therefore advisable.

What good practice guidance is available? The recently published revision of the Colombian National Cybersecurity Policy (CONPES 3995 - July 2020) included an implementation roadmap with specific actions to be carried out to achieve the strategic goals. These included: workforce development, different training courses and strategic exercises around digital security, as well as the development of activities to support and promote CSIRTs. OAS-Colombia's long history of partnership made the OAS/CICTE Cybersecurity Program as the best option to support the Colombian Government in the implementation of their NCS.

TOP TIPS

- Identify goals and objectives.
- Define a road map to implementation.
- Identify parties responsible.
- Assign a budget.
- Regularly monitor the agreement implementation.

COST AND DURATION

Cost: $260k USD approx.

Duration: 1 year.

CASE STUDY

With more than 15 years of experience, the OAS/CICTE Cybersecurity Program has become a regional leader in the support of OAS member states in the development of technical capacities and cybersecurity policies to prevent, identify, respond to, and successfully recover from cyber incidents.

In 2020, the OAS/CICTE Cybersecurity Program signed an agreement with the government of Colombia to collaborate on the implementation of the second review of their National Cybersecurity Policy. This model focused on the key areas of the strategy which the government believed could benefit from external expertise to address the stated goals.

This collaboration is divided into four (4) components and seven (7) activities.

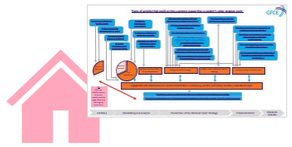
Component 1: Elaboration of the strategic vision for the implementation of actions of the national trust and digital security policy. This component took into account the creation of a Digital Security governance model in the country and the preparation of a methodological guide for the identification and management of digital security risks in adopting new technologies, such as, Internet of things (IoT), blockchain, Big data, Cloud Computing, Artificial Intelligence (AI), etc.

Component 2: Development of skills (workforce development), built on some existing initiatives of the OAS and support was given to organize a national virtual meeting of the Cybersecurity Innovation Councils which brings together regional experts and specialists in Design Thinking to promote innovation, raise awareness among citizens and disseminate best practices in cybersecurity in the region. Additionally, there is a target to train at least 500 public officials from public entities of the government of Colombia in information security under this component.

Component 3: Strengthening capacities for the Government's Cyber Incident Response Team (CSIRT) seeks to expand the capacity of the national CIRT through the provision of specialized technological services to strengthen cyber attack prevention mechanisms to critical web portals and services of 50 Colombian Government entities.

Component 4: Digital security capabilities with a differential approach, focuses on reimagining the delivery of capacity building especially in the current climate. As such virtual courses on cybersecurity, which include cyber exercises, focus on youth and students, preferably from low-income communities in the country, as well as on gender inclusion in order to exchange information, strengthen technical capacities in cybersecurity, and promote more inclusive career opportunities in cybersecurity, will be organized.

Overall, this approach to implementation makes the targets specific, measurable and time sensitive and can help a government become outcome oriented.



(19) Projects specific to capacity themes (e.g. CSIRTs; CIIP; Crime…)

ACTIVITY SUMMARY

What is the aim? To establish actionable, service-based internal, sectoral, and national CSIRTs and SOCs for governments and organizations.

Why do it? The benefits of creating CSIRT/SOC are the following:

- Manageable, coordinated and competent one-stop centers to deliver cybersecurity services for its constituencies;
- Effective, efficient and integrated cyber incident detection, response and recovery services to the constituency;
- Applied best international practice in a form of technology selection, delivery, operations, maturity assessments and roadmaps;
- Maximized Return on Investments (ROI);
- Recognition and trust among cybersecurity community locally and internationally.

What are typical outputs?

Depends on the scope/scale of the project, but typical outputs may include: initial assessment of CSIRT maturity level; preparation of design and implementation plan; creation of SOPs; design and implementation of technological solutions; extensive knowledge transfer via hands-on training and supervising of activities, etc.

How is it delivered?

Depending on the scope/scale of the project, the modus operandi may include:

1. Performing initial assessment 2. Preparation of a detailed CSIRT/SOC design and implementation plan 3. Preparation (review) of CSIRT/SOC mandate 4. Preparation of technical solutions architecture along with identification and proposal of alternatives for most suitable components 5. Preparation of essential policies and procedures 6. Implementation of technology solutions 7. Training sessions for staff 8. Soft launch 9. Update and upgrade of security operations 10. Official launch 11. Continuous support after the launch.

How easily can a country do it themselves?

As a result of legal obligations, countries often do it themselves using available guidance and resources. However, the process can become very lengthy and may be overshadowed by political divisions and biases before reaching the effective stage. NRD Cyber Security brings to the table an open-minded approach based on cost-benefit analysis and creation of results-driven services for the customer.

What good practice guidance is available?

ENISA's Guidelines for Establishing CSIRTs and SOCs, 2020; ENISA's "CSIRT Setting up Guide", 2006; ENISA's "Good Practice Guide for Incident Management", 2010; FIRST.org's CSIRT Services Framework

TOP TIPS

Effective Integration of the following vital components are the key for success:

Governance: Mandate definition along with roadmap and strategy preparation.

People/skills: Providing skills for incident detection and response, threat hunting and digital forensics.

Processes and services: proper planning of services and processes, process automation and reporting, standard operating procedures.

Technologic capability: e.g. automation of ticketing, information collection, processing and sharing.

Measurements: KPIs, SLAs, applying international best cybersecurity practices, such as SIM3 or SOC-CMM models.

International recognition: Assessments and introduction to Forum of Incident Response Teams (FIRST.Org), TF-CSIRT community.

COST AND DURATION

Cost: Depends on the scope/scale and complexity of the Project (is hardware and commercial software part of scope, as example), it often varies from 90k to 2000k USD.

Duration: Depends on the scope/scale of the project. Duration could vary from 9 months to 36 months.

CASE STUDY

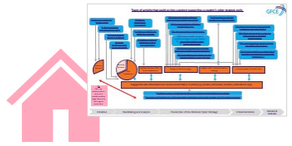
Digitization is progressing fast in Bangladesh and Bangladesh is now one of the emerging Asian destinations for sourcing software, information-technology enabled services and business outsourcing.
Bangladesh's new economy, largely based on the development of the IT industry, is expected to improve the socio-economic condition and livelihood of people. Therefore, the government is working to create the conditions for the businesses and citizens to act in a secure and non-toxic digital environment.

In 2016, Bangladesh Computer Council (BCC) initiated a project "Leveraging ICT for Growth, Employment and Governance Project (LICT)", financed by the World Bank, to improve Bangladesh's capacity to manage the risks related to the digital revolution and deal with fast-growing cybercrime. NRD Cyber Security was selected to implement this project and to establish Bangladesh's e-Government Computer Incident Response Team (BGD e-Gov CIRT).

In implementing the project, the NRD Cyber Security Team provided consultative and technical assistance which resulted in drafting mandates, regulations, applications and launching CIRT information systems while following ENISA, ISACA, Critical Security Controls and other methodologies.

Moreover, the supporting activities and deliverables included preparation of the government of Bangladesh Information Security Manual, Report on Bangladesh Information Security Classification and Information Protection Tools, Telecommunication and ISPs Information Security Manual, Cybercrime Legislation, cybersecurity awareness campaign and consensus building as well as the provision of CIRT training courses.

In the context of the project, a CMM assessment was also conducted (See activity 1).



(20) Projects specific to managing change (strategic communications, stakeholder engagement…)

ACTIVITY SUMMARY

What is the aim?
To ensure that the general public is aware of the government's cybersecurity priorities and objectives, to support any effort to raise cybersecurity awareness, and to communicate and promote opportunities for further engagement and cooperation with civil society and the private sector.

Why do it?
For a strategy's success and its accountability, it is crucial that stakeholders in all sectors but also the general public are aware of the NCS, its aims and the actions taken to implement it.

What are typical outputs?
A communication strategy is developed which defines the purpose, aims, objectives and activities, and a communication plan is implemented.

How is it delivered?
Activities include but are not restricted to: press conference, press release, validation workshop with stakeholders, publication of strategy on a publicly available website, as well as social media activities. Those are coordinated to ensure that the messages reach the audience.

How easily can a country do it themselves?
Easily. The country can work with the communications/PR team of the agency which is in charge of the NCS. Resources will be required for the implementation of some activities, but many can also be done with existing resources (website, social media accounts, meeting rooms).

TOP TIPS

- Get key stakeholders involved throughout the drafting process so they become ambassadors for the strategy through ownership
- Use existing resources and expertise in your organization such as the communications/PR department/team
- Choose a set of communication channels, e.g. traditional media (newspaper, radio, TV), social media, presentation, workshops to achieve reach
- Establish cooperation between key stakeholders for creating a broader outreach and creating media plans
- Have a lifecycle plan for the different stages to create attention from the beginning of the drafting, to the release of the strategy, and the time after
- Never let a good opportunity be wasted for getting attention for the strategy

COST AND DURATION

Cost: depending on the activity and the local conditions

Duration: the activities should take place in a coordinated and strategic way over several weeks to achieve reach and create impact. Have a lifecycle plan for the different stages to prolong attention about the strategy.

CASE STUDY

A national strategy that targets a wide range of stakeholders must also ensure it gets these stakeholders' attention and that the strategy is perceived as relevant among them, as this will increase the likelihood of successful implementation.

In Norway's case, when developing their 4th national cybersecurity strategy, the process was seen as just as important as the strategy itself. By having an open and inclusive strategy process, Norway sought to create ownership of the strategy by a large group of stakeholders. An ambition early on was to truly make it a national strategy for society, not only for the public sector: an open and inclusive process where everyone could contribute with ideas and input was considered as one of the main success factors to increase the likelihood of the strategy being perceived as relevant for the different stakeholder groups.

To gain a head start and to get attention from the very beginning, the strategy drafting process was launched with a strategy conference that was opened by the Prime Minister. It was important to get the target group's attention from a very early stage, and to include everyone that was interested in contributing. The event was thus open to everyone who wanted to attend and saw the involvement of over 300 delegates. Written input and high participation in a range of workshops clearly indicated that there is great interest in identifying shared solutions. Subsequent workshops with participation from both the public and private sector were also used to follow up on various target groups and prioritized areas. Drafts of the strategy were shared openly in these workshops for further input and discussions in order to include stakeholders throughout the different stages of the strategy process.

There is no use in having a good strategy that nobody knows about. Therefore, an integrated part of the strategy process was to develop a media plan to draw attention to the process. The media plan was developed in cooperation among selected ministries and agencies. This was crucial in order to make sure the strategy got attention and was successfully implemented in the wider community. Cybersecurity is a joint responsibility and concerns everyone. This should be reflected in both creating and implementing a national strategy.

A separate strategy launch conference was organized to increase attention for the release of the strategy. The Prime Minister of Norway, Minister of Public Security, Minister of Justice and Immigration, Minister of Defense and Minister of Research and Higher Education played a vital part in the conference and presented different parts of the strategy. This showed that the challenges we face are cross-sectoral and a key priority for the whole government. This open event was fully booked within a day, and the conference was livestreamed to gain as much attention as possible, resulting in over 1000 people following the launch of the strategy.

In addition, it was key to focus on using media and events to attract attention to the strategy in the time after its release. Building on the good cooperation between key stakeholders and utilizing their different outreach potential was seen as an important success factor for gaining broad attention.