NATIONAL STRATEGIES

INTERVIEWS BEHIND THE COVER

GFCE
Global Forum on Cyber Expertise

GLOBAL FORUM ON CYBER EXPERTISE 2018

Sharing good practice through the GFCE Working Group for Policy and Strategy

Norway is preparing its fourth national cyber security strategy in 2018. Robin Bakke explains why he wants it to be the most open strategy process ever.

Mexico published its strategy after consultation with a range of stakeholders. Carmen Valeria Solis Rivera advocates this inclusive approach that takes into account global good practice, as well as local context.

Senegal found careful planning and communication across the public and private sectors to be key in determining its strategy, according to Racky Seye Sambe

www.thegfce.com

STRATEGI

Over a very short space of time, the internet has altered the global landscape of which Norway is a part. We are seeing a sharp increase in digital security challenges and vulnerabilities. Norway's economy and security are dependent on a well-functioning global internet and robust digital infrastructure.

Børge Brende,

Former Minister of Foreign Affairs

Norway

NORWAY: A VERY OPEN PROCESS

AS NORWAY PREPARES ITS FOURTH NATIONAL CYBER SECUIRITY, THE PROCESS COULD BE MORE IMPORTANT THAN THE CONTENT OF THE FINAL DOCUMENT

Norway may have more experience writing national cyber security strategies than any other country – it is currently drafting its fourth – but it still looks internationally for advice and ideas. The man responsible for leading its latest strategy update is Robin Bakke, a civil servant in the Ministry of Justice and Public Security and the Norwegian representative to the Global Forum on Cyber Expertise. I interviewed him ahead of the GFCE Annual meeting to ask how he approached the task and what advice he had for others working on national cyber security strategies.

Norway wrote its first national cyber security strategy in 2003, putting it in the first wave of countries to do so. The government decided to prepare a strategy after an independent committee, looking into all national vulnerabilities, identified cyber security as an emerging critical issue. This use of an independent committee is part of Norway's strong culture of listening to academics, business and civil society when developing policy. They have continued to apply this approach. In 2015, another independent committee reported on Norway's digital vulnerabilities. The Ministry of Justice and Public Security followed this with their first White Paper on Cyber Security in 2017, which paved the way for a national strategy update in 2018.

Even though more than 100 organisations had already fed into the independent committee's report on vulnerabilities, Robin still wanted more external advice on the issues and solutions. His team held a national conference, opened by the Prime Minister, and then gave all stakeholders an opportunity to input into the strategy. He invited all stakeholders who submitted

suggestions to attend several workshops where the draft was openly shared for comments and further input. Robin wanted to run "the most open strategy process ever".

Although Norway had 15 years of cyber strategy experience, it still wanted to learn from international good practice and other countries. Robin mapped the key issues in other national cyber security strategies and spoke with ENISA, OECD, the NATO Cooperative Cyber Defence Centre of Excellence and the cyber policy makers in neighbouring and peer countries. Several international partners were invited to comment on Norway's 2012 strategy and their planned approach for the 2018 strategy. Robin said,

> "Using the international community helped a lot"

He met several people who had drafted national strategies who he thinks would be willing to offer advice to others going through the process.

Robin's team also spent a lot of time consulting and coordinating across the Norwegian government. Norway wanted to follow the good practice of having a strategy that covers both the civilian and military aspects of cyber security. To achieve this, the strategy was co-owned and co-written by the Ministry of Justice and Public Security and the Ministry of Defence. All ministries were asked to contribute with policy ideas. The team also reviewed the implementation of the last strategy, from 2012, and used Norway's annual risk reports produced by the national security agencies.

Consulting so widely within and outside government took time: the team began in December 2017 and they will send a draft strategy for ministerial approval in the near future. However, in Robin's opinion the process they followed was as important as the content of the final document. Through the process the team built national support for the strategy. This enables a devolved approach to strategy implementation that contrasts with countries who drive implementation by centralising their cyber security budgets or functions.

An inclusive strategy development process on its own is not enough to guarantee that a strategy will be implemented. Therefore Robin and his team are considering having a large, multistakeholder launch conference to put energy into the implementation from the start. It will then ask ministries to report progress at certain intervals. The Ministry of Justice and Public Security can insist on this reporting because they have the authority to audit other department's civil security preparedness. In other countries, such authority and influence might be held by the centre or a different security ministry.

Other ways in which Norway's approach might differ from other countries' include taking a decision to separate the action plan from the strategy and not putting an end date on the strategy. In Robin's opinion, making the action plan a separate document and process results in a better product and allows the plan to be adjusted more frequently.

Norway's action plan has two parts: an overview of government investments and initiatives that address the vulnerabilities that the strategy identifies; and a set of measures and guidance to help and encourage private and public organisations to improve their

Robin Bakke, Ministry of Justice and Public Security

own ability to prevent and manage cyber incidents. The goal is to raise the security level across the nation. Not giving the strategy an end date means the timing of Norway's next cyber strategy will be driven by changes to real world conditions and not a date in the calendar.

For the first time, Norway's strategy aims to fully incorporate the international dimension. This follows the Norwegian Ministry of Foreign Affairs writing a first International Cyber Strategy in 2017.

Asked for his top tip Robin said,

"The most important thing is to use the process to set a common direction for the country and, through this, to align all stakeholders to implement the strategy and support each other…. and make it short and attractive!"

Whether you are a large country drafting your fourth national strategy or a small one drafting its first, these are good practices we should all follow.

By Robert Collett, FCO UK

MEXICO:

A MULTISTAKEHOLDER APPROACH

CARMEN VALERIA SOLIS RIVERA, DIRECTOR FOR DRUGS AND CYBER SECURITY AT THE SECRETARIAT OF FOREIGN AFFAIRS OF MEXICO, GIVES US AN OVERVIEW OF HOW MEXICO DEVELOPED ITS NATIONAL CYBERS ECURITY STRATEGY (NCS) IN 2017.

Despite earlier attempts to develop a cyber security strategy for the country, it wasn't until early 2017 that the Mexican government decided to put the NCS development process in motion. It was at this point that the key components, such as growing internal challenges in dealing with cyber threats, good practice in other countries in the region, access to external expertise, and the government's determination, fell into place and provided an enabling environment to kick-start the process.

The support of the international community and the influence of global and regional good practice were key triggers in creating this favourable international context.

When the Organization of American States (OAS) approached the government of Mexico to offer their technical support to facilitate the process in early 2017, it was clear that the country did not want to lag behind international and regional trends. Other countries in the region had just recently published their NCSs, following a global trend of NCS development in countries around the world.

ESTRATEGIA

El objetivo general de la Estrategia Nacional de Ciberseguridad es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano.

In response, the Office of the Presidency, with its versatile and dynamic team, decided it was time to take the lead and assumed the coordination tasks. Looking back, the central involvement of the executive proved to be a main factor in its success, as it ensured leadership and buy-in across government. Another key factor was the supporting role of the OAS, which brought first-hand experience and expertise to the table, and helped to set out clear guidelines and timetables for the process. Furthermore, the OAS's 2016 report "Cyber security – Are We Ready in Latin America and the Caribbean?" served as a baseline assessment of the country's cyber security maturity levels, and provided a starting point for the content of the NCS.

Working alongside the Ministry of Foreign Affairs, and supported technically by the OAS, the Office of the Presidency organised the first official workshop in April 2017. The event brought together key stakeholders from across government, as well as other stakeholders, such as the OAS, ICANN, and the OECD, as well as the governments of Canada, the US, Spain, Colombia and Chile.

By inviting international experts to provide input into the workshop, Mexico's NCS process benefited from their guidance, advice about potential challenges, and examples of good practice and avoidable failures. Lessons learned from a preceding wave of NCS development across the region, notably Chile and Colombia, were particularly valuable. The outcome of the workshop was a report with official recommendations for the development of the Mexican NCS.

Follow-up sessions were held during June and July, which aimed at consolidating the contributions generated in the first workshop and in other national workshops. Furthermore, during these sessions the first draft of the strategy was discussions with key national actors, such as academics and legislators.

Throughout the process, strong emphasis was placed on multistakeholder engagement. This was exemplified by a formal public consultation on the draft NCS that was launched following the second workshop. The online consultation allowed all stakeholders, and especially end-users, to be involved in the process. In total, more than 80 comments were received and subsequently incorporated into the final text of the NCS. The comments contributed to the adjustment of the initial draft of the strategy.

Equally important were efforts made to embed durable institutional mechanisms for continued multistakeholder involvement through the ongoing follow up and implementation process. These measures, taken together, are seen to have provided a dual benefit: improving the substance of the strategy, while also fostering long-term buy-in across the Mexican cyber security community.

Officials from the Government of Mexico noted the importance of international good practice and its relationship to local knowledge and expertise. While the emerging global body of NCS texts, as well as guidance and input from veterans of processes in other countries, proved crucial in developing the process, they weren't in themselves sufficient.

To succeed, the strategy had to be intricately tailored to the unique local needs, concerns, and dynamics at play in Mexico. The role of good practice, then, is less as a toolbox of methods which can be applied "off the shelf" in any context, but rather as a resource which demands careful and rigorous unpacking and fitting.

Finally, from the government's perspective, the benefits of having gone through this process could not be overstated. The impact of the NCS has been multifaceted. It has helped consolidate the country's cyber security objectives, activities, and institutions, making it better prepared to address existing and emerging cyber security challenges; it has put Mexico's example on the international stage, creating new opportunities for outreach and collaboration; and it has added a rich example to the growing global body of good practice in NCS development.

By Lea Kaspar, Global Partners Digital

Carmen Valeria Solis Rivera, Director for Drugs and Cyber Security at the Secretariat of Foreign Affairs of Mexico

STRATÉGIE

La vision du Sénégal pour la cybersécurité s'intitule « En 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous ».

Afin de mettre en œuvre cette vision, le Gouvernement du Sénégal s'emploiera à atteindre les cinq objectifs stratégiques suivants :

1. Renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal

2. Protéger les infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal

3. Promouvoir une culture de la cybersécurité au Sénégal

4. Renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs

5. Participer aux efforts régionaux et internationaux de cybersécurité.

SENEGAL: A FIRST STRATEGY

SENEGAL USED A METHODICAL PROCESS TO DEVELOP ITS STRATEGY

Senegal developed its National Cyber Security Strategy as an outcome of the GFCE Initiative "Progressing Cybersecurity in Senegal and West Africa", which began in early 2017. A benchmark for the country's cyber security stance was established through the deployment of the Cyber Security Capacity Maturity Model (CMM) developed by the Global Cyber Security Capacity Centre (GCSCC). With the support of the Dutch government and the Commonwealth Telecommunications Organisation, Senegal then developed the strategy in a multi- stakeholder process, published in April 2018. Currently, the government is planning the implementation of the strategy, and is looking for partners to support the process.

The GFCE initiative which led to the strategy, "Progressing Cybersecurity in Senegal and West Africa", includes collaboration with the Government of the Netherlands, the Senegalese Ministry of Postal Services and Telecommunications, the GCSCC, and the United Nations Office on Drugs and Crime.

Racky Seye Samb, from the Ministry of Communication, Telecommunications, Postal Services and the Digital Economy, was part of the process from the beginning. She believes that membership of the GFCE, the launch of this initiative, and the early political buy-in created a strong starting point for the strategy. The establishment of trust and buy-in from the start continues to be a key factor in the ongoing commitment by the government and other stakeholders involved in the initiative. The strategy was also based on the National Digital Strategy, which states that digital confidence is one of the prerequisites for the digitalisation agenda, and that the development of a strategy is a priority.

The first activity of the GFCE initiative in January 2016 was the cyber security review, based on the CMM, which enabled Senegal to analyse its own cyber security situation.

The capacity review, which was validated by a diverse range of public, private, and civil society stakeholders who participated in the process, provided the government with the evidence needed to take the next steps. As the strategy development was one of the main recommendations, the Minister and Presidency approved the drafting process shortly thereafter.

After the review, the Ministry of Communication, Telecommunications, Postal Services and the Digital Economy started the strategy drafting process. The Senegalese government mandated the Ministry to lead this work. The Ministry created a cyber security working group, including government, private, and civil society representatives, to prepare for the review and then lead the drafting process. With the support and assistance of the GFCE and the Commonwealth Telecommunications Organisation, the strategy was drafted over three months.

The national capacity review provided the baseline data for developing strategy content. The government aligned all projects in the strategy with the review's recommendations. The strategy development process was also aligned with national risks, priorities and objectives. Capacity building is one of the objectives of the strategy, and investment in security is the key driver of the strategy implementation.

A number of stakeholders were invited to participate from the beginning and stayed involved throughout the drafting process. These stakeholders included organisations from the public and private sectors and civil society members who work inside the cyber security domain, such as the army, law enforcement, data protection institutions, and NGOs. It was seen as a priority for the lead ministry of the strategy to demonstrate leadership by keeping these stakeholders involved throughout the process and by building and maintaining trust.

The government looked at international good practices from countries, such as Ghana and New Zealand.

The government decided it was important to involve the private sector, because they own much of Senegal's critical national infrastructure. They made it clear that the private sector should be involved in the national cyber risk management process and work with the National ICT Agency.

Finally, the strategy was approved by the Cabinet and President and was published in April 2018. The budget for developing the strategy came from the Ministry itself, which was mainly to fund the workshops that were part of the process.

Challenges during the drafting process included language barriers, as most stakeholders are only or mostly confident in French, and many of the supporting materials and good practices are in English.

Senegal is now ready to start the implementation of the strategy. The plan is to create a new cyber security task force that will coordinate the activities and define the roles and responsibilities of each stakeholder. It will also monitor and evaluate progress. In addition, the task force will promote the implementation process among stakeholders, and ensure that they continue to stay involved in all planned activities.

However, currently the biggest issue is identifying which institution will take the lead for the implementation process and create the task force. At present there is no budget to implement the strategy in Senegal. The government is looking for partners to support the country in this regard.

By Carolin Weisser, Oxford Martin School

Racky Seye Sambe, Ministère de Communication des Télécommunications Des Postes et de l'Économie Numérique, Sénégal

Lessons Learned:

The importance of involving the private sector. As they own major parts of national infrastructure in Senegal, as in other countries, they are concerned about cyber security issues.

The need to facilitate public-private partnerships, as this is important for investments in cyber security and the commitment to the NCS.

It is crucial to raise awareness of cyber security related issues among national authorities.

For a country with a low awareness of cyber security, starting out with a strategy first requires a complete capacity review to understand the gaps and the areas for capacity building.

Needs and Expectations towards the GFCE:

Assistance for partners to run workshops.

Knowledge and expertise on Cyber Diplomacy.

Advice on the way forward for the implementation of the strategy.

Metrics to evaluate the effectiveness of a strategy.

REFERENCES:

NORWAY:

2015 Committee on Digital Vulnerabilities Report - https://tinyurl.com/norstrat2

White Paper - https://tinyurl.com/norstrat1

MEXICO:

Mexico's National Cybersecurity Strategy -
https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

"Cybersecurity: Are we ready in Latin America and the Caribbean?" -
https://publications.iadb.org/handle/11319/7449

Recommendations for the Development of the National Cybersecurity Strategy, OAS Technical Assistance Mission - https://tinyurl.com/OASrec

Open consultations on the NCS draft -
https://www.gob.mx/participa/consultas/documento-ciberseguridad

Consolidated input from national actors on the NCS. – https://tinyurl.com/NCSinput

SENEGAL:

Senegal CMM Report -
https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/senegal-cybersecurity-capacity-review-2016

Senegal National Cybersecurity Strategy -
http://www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf

GFCE initiative "Progressing Cybersecurity in Senegal and West Africa" -
https://www.thegfce.com/initiatives/p/progressing-cybersecurity-in-senegal-and-west-africa

GENERAL:

Cybersecurity Capacity Maturity Model for Nations (CMM) -
https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

GFCE
Global Forum on Cyber Expertise