Global Good Practices

November 2017

DiPLO

GFCE
Global Forum on Cyber Expertise

Table of contents

Introduction

The Global Forum on Cyber Expertise (GFCE) was launched at the 2015 Global Conference on Cyber Space (GCCS2015) in The Hague, to strengthen cyber capacity and expertise globally, while upholding the values of an Internet that is free, open, and secure. The GFCE is a global platform for primary stakeholders to exchange good practices and expertise on cyber capacity building. Its objectives are to identify successful policies, practices, and ideas, and to multiply and leverage these on a global level. In preparation for the 2017 Global Conference on Cyber Space (GCCS2017) in New Delhi, India, the GFCE prepared a Roadmap to guide the development of a long-term, global cyber capacity building strategy. The Roadmap defined two documents to be prepared and presented at GCCS2017 as building blocks for this longer-term strategy: a **global agenda for cyber capacity building**, which identifies future priorities; and a set of **global good practices** (GGPs) on a variety of cyber topics.

Collecting the global good practices

GFCE members work together on several practical initiatives to build cyber capacity. The capacity building work done in recent years by GFCE members and partners, both within these initiatives and beyond, provides a rich set of experiences and knowledge. Collecting and sharing GGPs will ensure that other cyber capacity building initiatives can benefit from this experience and expertise in their own efforts.

The process of identifying and collecting GGPs (described in detail in the Methodology section) started with the GFCE initiative's teams and coordinators. Each team identified potential practices to be included in the collection of GGPs. Through discussion and analysis, the teams, with the support of DiploFoundation, narrowed down the selection and prepared a detailed description of each chosen practice. Participants in the process brought with them years of experience and practice in cyber capacity building from within and without the GFCE. The candidate practices were examined in the light of capacity building theory and practice from the development sector. The GFCE community was invited to read and provide feedback on the draft collection of GGPs, which helped further refine the resulting document. This reflective and collaborative process of identifying, analysing, and describing the GGPs ensured GFCE community ownership of the collection and a better knowledge for all about the work done by the many GFCE initiatives.

This document presents the outcome of this process: a collection of identified global good practices from the GFCE.

Objectives of the document

The collection of GGPs was developed as a practical reference tool for various actors working to build cyber capacity. It should:

Raise awareness of effective practices in the cyber capacity building field.
- Identify practices which may be extended or replicated on a global scale, or in other wregional, national, or local settings, with appropriate adaptation.
- Offer inspiration, practical guidance, and concrete steps, based on tested and proven practices, for stakeholders from various sectors, with different levels of expertise and background, to improve their own practices and contribute to global cybersecurity.
- Facilitate further partnerships and knowledge sharing in the cyber field, particularly through the GFCE.

Who this document is for, and how it could be read

This document is aimed at the different stakeholders that take part in cyber capacity building:

- Governments, including policymakers, decision-makers, regulators, and other public authorities
- Law enforcement authorities, including police and prosecutors
- Expert communities, including researchers, academics, and technical communities
- CERTs, CSIRTs, CIRTs, and ISACs
- Private sector, including IT businesses, Internet service and hosting providers, content providers, and vendors
- Civil society, including NGOs and end-users.

The GGPs are presented in a catalogue. Each GGP includes a short general description, the main stakeholders involved and targeted, some reflections on the broader capacity-building context of the practice, instructions on how to replicate or join it, examples of where the practice was successfully used, and additional resources and contacts.

While the document can be read linearly, each GGP can also serve as a stand-alone resource. Each user can select and read the GGPs of personal interest. To make it easier for particular stakeholder groups to navigate the collection of GGPs and find what is of interest for them, each GGP is tagged by key stakeholders to whom it should be of primary interest (although other stakeholders may benefit as well and are certainly encouraged to read through), and by the main thematic areas to which it is related (the same themes used in the *Global Agenda for Cyber Capacity Building*), to enable an easier matching of agenda priorities with specific practices. In addition, each GGP is accompanied by a hashtag as a short version of the title, to enable easier referencing throughout the document.

The visual navigation maps, available in the annex and presented briefly immediately before the collection of GGPs, should assist each of the stakeholders to pick thematic areas of interest and navigate directly to related GGPs.

Methodology

The process

Collecting the GGPs took place through several phases, conducted from May to November 2017, facilitated by a research team from DiploFoundation.

Preparing a research framework

The theoretical and practical background of capacity building in cyber and non-cyber fields was analysed. A framework for review of the initiatives was created, which covered current good practices and important dimensions in capacity building (based on research and practical experience in the capacity building field). The framework facilitated the gathering of important information about each initiative:

- What is the purpose of the capacity building initiative (how is capacity defined, whose capacity, capacity for what)?
- Which stakeholders are involved?
- What levels does the initiative work at (international, national, networks, organisational individual)?
- Which types of capacity does it aim to develop (hard capacity, soft capacity)?
- What are the relevant aspects of the implementing environment (organisational culture, political context)?
- How is the work being monitored and evaluated? What results have been seen so far?
- What potential is there for replication?
- What are the specific activities undertaken on the different levels where the project operates?

Discussing the research framework and matching it with the work of Initiatives

Key concepts and the research framework were discussed with the initiative teams and coordinators at the GFCE meeting in Brussels (May 2017). Initiatives were reviewed through this framework, both through reading available documentation, and through discussion with the initiative coordinators. This review provided an initial broad understanding of each initiative.

Identifying candidate practices

Next, the initiative coordinators were asked to identify potential candidate practices to be included in the collection of GGPs. The coordinators filled out a questionnaire, describing each identified practice, explaining how and why it works, and providing recommendations for implementation. This was followed by a voice interview (usually about one hour long) and further discussion via e-mail. Through this interaction, the initiative coordinators and Diplo identified and selected several good practices for each initiative for inclusion in the collection.

Drafting the proposed good practices

As a basis for identifying and describing the set of good practices, the information gathered about each GGP was analysed within the framework of good capacity-building practices from the development community, and known needs and gaps in the cyber field. To ensure the good practice could also be global, the potential for replication was assessed (if/how these practices could become global, or could be implemented in different locations with different political and cultural contexts).

The research team prepared a detailed description of each practice which included:

- A 'teaser' to catch the interest of the readers.
- A short description, suitable even for readers without deep experience of the field.
- A section called 'the big picture', providing the wider context and anchors to capacity building.
- Instructions and specific steps to be undertaken by implementers interested in replicating it.
- A possible timeline for implementation
- Specific examples from the work of a GFCE initiative.
- Creative illustrations, where possible, to highlight the main message in visual form.

The drafts were then shared with the initiative coordinators and refined through their comments and feedback.

Gathering community reflections

Following feedback from each initiative, the draft full collection of GGPs was shared with the broader GFCE community, to invite further suggestions and feedback. Feedback received from each initiative and from the GFCE community was incorporated into subsequent drafts. The GFCE meeting in The Hague (September 2017) provided further opportunities for discussion and consultation on the draft GGPs, with particular focus on how to best present the GGPs to various audiences so that each stakeholder could find what is of particular interest.

Compiling the final report

While compiling the final report, several insights emerged related to how capacity building in the cyber field is accomplished effectively. These were formulated as a chapter on cyber capacity-building highlights. A set of visual maps was prepared to help readers to navigate through the collection of GGPs more easily. Finally,

the initiatives and their GGPs were showcased in this report, which should serve as a useful reference document for various actors in the cyber field who can seek inspiration from practices that have proven effective and may be replicable. The report aims to facilitate further partnerships and knowledge sharing in the cyber field.

Main concepts

Some concepts used frequently throughout the report include:

Global good practice (GGP)

A GGP may be defined as a good practice, recognised by experts in the field, which, having been proven to work and produce good results, is generically applicable for the global community. For example, a GGP might be a practical tool, basic standards, or a guideline document.

Capacity

According to the UNDP[1], capacity is the ability of individuals, institutions, and societies to perform functions, solve problems, and set and achieve objectives in a sustainable manner.

Capacity development

The ECDPM[2] defines capacity building as the process of enhancing, improving, and unleashing capacity; it is a form of change which focuses on improvements.

The UNDP[3] defines capacity development as a process through which individuals, organizations and societies obtain, strengthen, and maintain the capabilities to set and achieve their own development objectives over time

The OECD[4] understands capacity development as the processes whereby people, organisations and society as a whole unleash, strengthen, create, adapt and maintain capacity over time.

With regard to terminology, it is important to note that the authors recognise that some organisations differentiate between capacity development and capacity building. In this report, however, the two terms are used with the same meaning, and we assume that both processes recognise and build on existing capacity.

---

[1] UNDP (2009) Capacity Development: A UNDP Primer. Available at http://www.undp.org/content/undp/en/home/librarypage/capacity-building/capacity-development-a-undp-primer.html [accessed 15 November 2017].

[2] Baser H and Morgan P (2008) Capacity, Change, and Performance: Study Report. ECPDM Paper No. 59B. Available at http://ecdpm.org/publications/capacity-change-performance-study-report/ [accessed 15 November 2017].

[3] UNDP (2009) Capacity Development: A UNDP Primer. Available at http://www.undp.org/content/undp/en/home/librarypage/capacity-building/capacity-development-a-undp-primer.html [accessed 15 November 2017].

[4] OECD (2006) The Challenge of Capacity Development: Working Towards Good Practice. Available at http://www.fao.org/fileadmin/templates/capacitybuilding/pdf/DAC_paper_final.pdf [accessed 15 November 2017].

Cyber capacity building highlights

This research focused on identifying good cyber practices used by the current GFCE cyber capacity-building initiatives. This collection of good practices will facilitate extending current capacity-building efforts through raising awareness of what the actors in this field are already doing effectively.

The process of researching, analysing, and compiling the GFCE GGPs produced several insights related to how capacity-building activities and programmes in the cyber field are accomplished effectively. These insights have been formulated as a set of **cyber capacity building highlights**. The highlights listed were drawn from the GFCE initiative's GGPs, and are presented together with examples of source GGPs. They also align with principles and approaches to capacity building advocated by the broader development community and especially with the guiding principles for cyber capacity building identified in the Global Agency for Cyber Capacity Building.

1. Inclusive partnerships and shared responsibility: Effective cyber capacity building requires cooperation across nations, including various stakeholders, and at different levels

2. Ownership: Partner nations need to take ownership of capacity building priorities

3. Sustainability: Obtaining sustainable impact should be the driving force for cyber capacity building

4. Trust, transparency and accountability: Transparency and accountability play a key role in establishing trust, which is necessary for effective cooperation

How are these highlights useful?

- They illustrate how current cyber practices align with good practice in the broader development field.
- They can help practitioners to effectively adopt and adapt the GGPs to new contexts through focusing on the underlying principles and approaches which are valid in a wide range of environments, rather than the details which are specific to a particular context.
- They can help guide the development of new practices, which may be innovative yet based on tested and proven principles or approaches.
- They may help to identify innovations that the cyber field brings to the broader capacity building field, due to its transformative effect on society and the economy.

1. An inclusive, multistakeholder approach to capacity building is required.

Due to the complexities of the topic and roles that various stakeholders play in cyberspace, capacity building initiatives need to involve relevant stakeholders (governments, international organisations, civil society, academia, industry, etc.) and work at different levels, from the international down to the local. In this regard, determining which stakeholders should be involved, and at which levels, is an important early step.

- The review of a country's cybersecurity maturity and readiness requires multistakeholder engagement (***#MaturityModel***).
- A voluntary-based cooperation platform, that gathers various stakeholders and has a common goal and shared responsibility, can ensure an increased level of security through raising awareness about weaknesses in systems (***#MSPlatform***).

2. Capacity building resources developed by partnerships of stakeholders engaged in delivery will be more comprehensive and useful.

Guidelines, good practices, and training materials, developed by the technical community and the private or public sector, should be integrated into existing capacity building programmes.

- For instance, training materials to assist mitigation of systemic vulnerabilities, developed as part of the measurement of network health, should be integrated into various existing programmes of capacity development institutions, ensuring a diversity of stakeholders to be targeted (***#Scorekeeping***).

3. Local ownership of the capacity building process is essential for effectiveness and sustainability.

In many cases this means that a partner beneficiary government makes the decision to carry out the activity, and take active participation, if not lead it. However, local ownership should not be imposed, but rather stimulated and encouraged.

- For instance, the government decides to conduct maturity assessment, decides on the composition of the team and invites participants, and decides about the use of the report and recommendations (***#MaturityModel***).
- Political commitment by the government to enhance capacities for combating cybercrime is what ensures, in most cases, an efficient local team and full support to capacity development in this field (***#NationalTeams***).

4. Sustainable capacity building requires a comprehensive approach.

Capacity building needs to be carried out in a systematic way, through multiple levels and dimensions.

- The review of a country's cybersecurity maturity and readiness requires a multidisciplinary approach (*#MaturityModel*).
- Statistically mature and vetted metrics about the health of the networks, if visualised, presented in a comprehensive manner, and published in reports about the health of the ecosystem, could be useful, not only in a technical context but also in a regulatory context or a context of international affairs, and used by governments, the private sector, and other stakeholder groups (*#HealthMetrics*).

5. Capacity building activities should recognise and build on existing capacities.

A variety of actors with stakes in cybersecurity bring numerous existing capacities, which should be mapped and used as a base for further capacity building.

- Existing capacities are assessed and understood before anyone can build on them (*#MaturityModel*).
- Training materials about good practices in the mitigation of network vulnerabilities should be integrated into various existing capacity building programmes through partnerships with capacity building institutions, to enhance the existing capacities and strengthen existing programmes (*#Scorekeeping*).

6. Development of soft capacities is often equally as important for the cyber field as hard capacities.

A multidisciplinary and multistakeholder environment demands mature inter-professional and intercultural communication skills, and often also negotiation skills, the ability to adapt and learn, to innovate, and be responsive to the changing environment.

- Developing a functional dialogue among stakeholders gathered on a voluntary basis, with a common goal and shared responsibility rather than opportunistic aims by various parties, requires particular skills (*#MSPlatform*)
- To make various metrics about the health of cyberspace useful to a diversity of stakeholders, including decision-makers, experts need to develop skills to present technical findings in a comprehensive – often visual – way (*#HealthMetrics*).

7. Establishing trust among stakeholders is an important element of capacity building in the cyber field.

Since securing cyberspace often involves the sharing of sensitive data about attacks or incidents suffered, existing vulnerabilities in systems, and successful response approaches, it is important that all actors feel comfortable in exchanging knowledge and communicating with partners at all stages of development relationships.

- Support for a capacity building programme can be provided through regional hubs – partner countries with already existing capacities – yet trust and good relations among neighbours are a precondition for such approach (*#RegionalHubs*).
- A free public service for testing the compliance of various Internet users with selected security standards can encourage individuals and organisations to use and comply, only if they can trust that the stakeholders behind the tool will not misuse it (*#TestingTool*).

8. Exchange of knowledge and practices is a key component of cyber capacity building.

The fast pace of development of new risks forces actors to build their own experience, sometimes from scratch. Even the most experienced actors find value in the experiences of their peers, while newcomers can avoid typical mistakes and leapfrog problems. Such an environment enriches the overall pool of experience and adds value to exchanges and communications.

- The clearinghouse that analyses weaknesses in networks needs to collect data from multiple sources of measurements in order to process it; on the other hand, the results and findings of these analyses need to be open, so that other parties can benefit from them (***#Clearinghouse***).
- Through sharing of experiences about awareness-raising campaigns, more experienced partners can reflect on their practices, while less experienced partners can move more quickly towards effective practice (***#Campaign***).

9. Awareness-raising is an important driver for cyber capacity building.

Complex as it is, the topic of cybersecurity is often seen as a technological issue, and there is a general lack of awareness about socio-economic aspects, especially among public institutions and the broader citizenry.

- An awareness-raising campaign related to cybersecurity contributes first towards engaging stakeholders and sharing a vision, then towards learning and improving the various capacities of the broadest constituency (***#Month***).
- Metrics developed by the technical community to track the health of cyberspace, presented in an easy and understandable way, can improve awareness among policymakers and state decision-makers about cyber-risks, and then increase the capacities of the decision-making level in corporations to assess risks and provide resources for mitigation (***#HealthMetrics***).

10. Real-world situations and simulations are particularly valuable for developing capacities in the cyber field.

Learning-by-doing is a common approach in other fields, not only cyber; yet the complexity of issues related to cyber and cybersecurity in particular often leaves no options to explain the risks and remedies but to run tests and simulations.

- A simple public online tool, like internet.nl, which tests the implementation of security standards in anyone's domain, e-mail, and connection, can both motivate further learning and be a guide for communities that exchange knowledge in the field (***#TestingToolkit***).
- Using the technical tools for monitoring improvements in the health of a network – scorekeeping – can also help identify various experiences and extend the collection of good practices for mitigation of risks (***#Scorekeeping***).
- Organisational capacities are also strengthened by assisting partners to work on particular practical activities such as awareness-raising campaigns (***#Campaign***).

Navigating through the GGPs

Readers are encouraged to read throughout the document. Since each GGP serves as a stand-alone resource, readers can also navigate directly to the GGPs of interest to them, by consulting the visual navigation maps (Annex II):

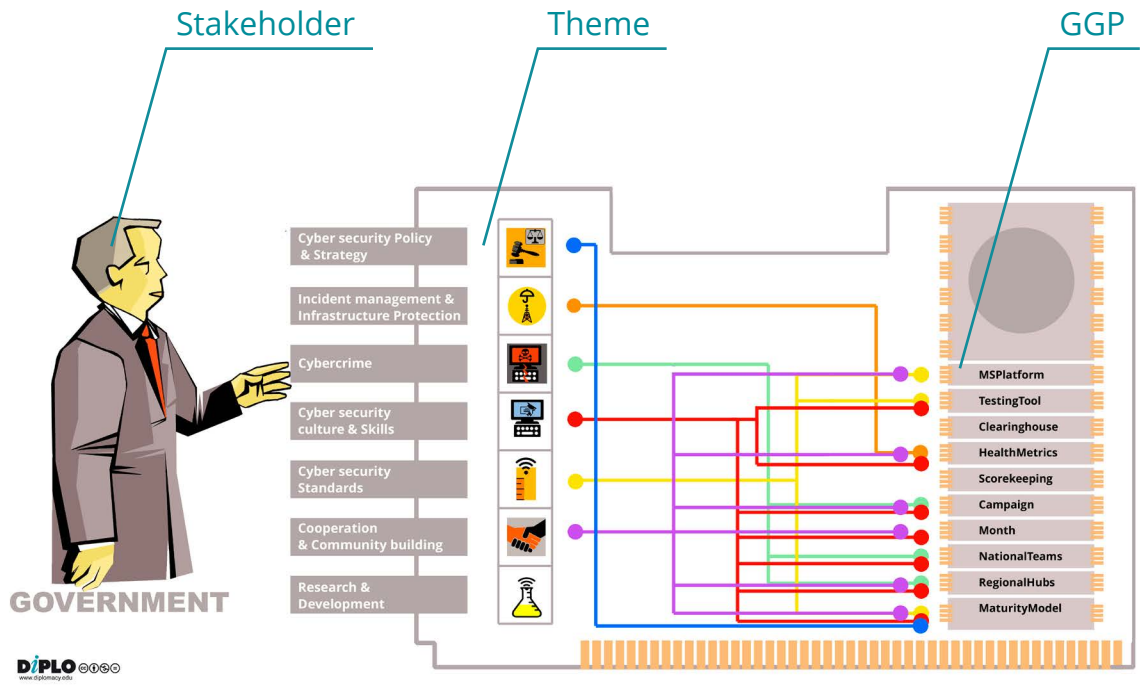
Step 1: Select the stakeholder group of interest

Step 2: Select the thematic area of interest

Step 3: Follow the lines (colours) from the selected thematic area to the related GGPs.

Step 4: Go to the chosen GGP to learn more about it.

Example:



Catalogue of GFCE global good practices

Practice: **Establish a national multistakeholder platform to promote standards**

#MSPlatform

"Better safe than sorry." Prevention means increasing the security of the system, including through implementing the latest standards. How can we make sure the right players are gathered to discuss the right things and support the community in the right way? A multistakeholder networking platform serves as a vehicle for initiating and coordinating efforts among partners, promoting and giving exposure to activities, and serving as a contact point for various players.

Related thematic areas:

Standards

Cooperation and community building

Of particular interest to:

Description

A voluntary-based cooperation platform, that gathers various stakeholders and has a common goal and shared responsibility, can ensure an increased level of security. Such a platform encourages partners to raise awareness about the weaknesses in systems, discuss main challenges and solutions, and provide support for preventive measures. This mechanism is transparent and triggers improvement, and its results are an incentive for organisations to do better.

The platform can set up test tools to identify weaknesses in systems (*#TestingTool*), organise webinars and workshops on certain topics for interested parties, and provide support to address weaknesses (through questions and answers, or a repository of how-to guidelines). If a member of the platform identifies a topic that could be useful to discuss, it is flexibly addressed.

The practice is focused on promoting the use of existing standards, rather than developing new standards.

Actors (or who this is for)

The platform formula stimulates multistakeholder cooperation and the sharing of expertise through its diversity. This is needed because the implementation of security standards is a collective effort by many parties.

A typical platform is comprised of technical Internet organisations and departments – the national CERT, the Ministry or NRA in charge of Internet policy-making, and umbrella organisations representing businesses in the ICT sector, for example ISPs, ICT solution providers, manufacturers, and hosting providers. There can also be other organisations that underpin and support the activities, as long as their participation is not driven by an individual commercial interest.

The big picture

Prevention is a fundamental aspect of security, and adhering to some of the many global standards is an important component. A specific regulatory environment that requires entities to implement leading security standards might not be the only – or the best – approach: economic interests can be an incentive for self-regulation. A voluntary-based cooperation platform which gathers various stakeholders – and particularly those that can ensure the implementation of particular security standards (such as the technical community and the private sector) – is also a valid instrument.

The platform contributes to the development of an enabling environment at national level, as institutions become more sensible to the need for existing Internet standards. It also contributes to partnership building by creating mechanisms and frameworks for cooperation and collaborative learning. It therefore develops the capacities of the involved parties through cooperation, awareness raising, focused workshops and discussions, expert support and advice, exchange of resources, and development of guidelines for deployment of standards.

Instructions

- Involve organisations and institutions particularly interested in the specific technical topic, such as security standards. Participation should have a low barrier – open to parties that support the mission and activities, and will not use the platform for product presentation or commercial reasons.
- Prepare and agree on a code of conduct which outlines the basic principles of participation.
- Find the most meaningful and feasible way of participation for each partner. Partners should contribute to the platform by offering the time of their employees involved in activities, hosting or facilitating meetings, or utilising their communication channels for outreach.
- Organise the platform as a lightweight 'organised network' rather than an organisation; it does not need a headquarters, employees, or formal partnerships.
- Avoid unnecessary overhead costs and bureaucracy. Ensure a basic budget – through contributions of several actors and possibly the government – for basic support (active chairperson, website and tools development, secretariat functions). Other contributions should be in-kind by partners.
- Focus the discussions and work on technology – challenges and solutions – rather than on broad aspects.

Some possible challenges in replication of this practice include:

- Different national playing fields need to be examined. In general, the platform formula works best in an environment that already is acquainted with and has experience of multistakeholder cooperation. In environments where a multistakeholder model is a new concept, a different approach might be considered.
- The biggest challenge is in the initiating phase. Most parties in the private sector acknowledge the need for action, but are not willing or do not feel the responsibility to take the necessary first step.
- A possible extension of the platform beyond borders would increase the number of requests for support, and a voluntary model of support with no budget would

not be feasible. It is therefore better if the model is adapted nationally, in different countries, to make it locally specific.
- As the GFCE membership comprises only states and companies, an extra effort is needed to reach out to Internet organisations, civil society, and umbrella organisations for ICT to cooperate on a national platform. The member state/regional organisation should therefore take on the role of approaching stakeholders in its respective country or region.

Timing

There is no general scheme or timescale for setting up a platform. It depends highly on the local environment. Drawing from practice in the Netherlands, it took about one year to set up an operational platform. New local initiatives could be set up faster, learning from the experience of other platforms.

Once established, the lifetime of a platform depends on the initial goal; for example the platform could dissolve when a certain percentage of implementation has been achieved. In principle, the platform continues to be useful as long as the implementation of standards does not achieve a certain maturity. For certain standards, this can take a long time. For instance, a similar task force for the promotion of IPv6 still exists after about 10 years, since the IPv6 roll-out is rather slow.

Example

The GFCE Internet Infrastructure Initiative follows experience in the Netherlands of testing and monitoring compliance with international Internet standards, and seeks to broaden this know-how. In this regard, a voluntary cooperation platform with targeted activities was established.

The Dutch government embraced the public interest of this initiative and became an active driving force in setting up the platform. It gave initial funding (being a majority financial contributor) and gathered interest and participation. Although still substantial, the government's involvement in terms of money and time spent has decreased after two years as a result of the increased involvement of other partners.

The platform focuses only on technical standards, specifically on standards of service. It is not being extended beyond these, as it mainly comprises technical organisations and departments.

The platform organises two seminars or workshops a year for interested parties. The events are narrowly focused – such as on e-mail security – covering implementation practices and tools, preferably open source, and how various tools complement each other. Another example is a paper on encryption and Transport Layer Security, also taking into account political aspects. Emerging issues, such as the pros and cons of Digital Objects Architecture, were also among the topics.

The number of companies and organisations involved in the platform has increased each year, and the platform has maintained the tempo of a minimum two seminars a year. The increase in the use of the testing tool (#TestingTool) drove more requests for support to the platform. There has been a general improvement recorded in the implementation of security standards across the Netherlands.

Source, support, and mentoring

Internet Infrastructure Initiative at the GFCE website: https://www.thegfce.com/initiatives/i/internet-infrastructure-initiative

Contact point:
Thomas de Haan (T.S.M.dehaan@minez.nl)

Practice: **Create a website for testing standards compliance**

#TestingTool

Proper use of the latest versions of Internet standards is a crucial element for a robust Internet infrastructure. There is generally no lack of standards, but it is important to stimulate, encourage and ensure stronger implementation. Is your Internet connection, website or e-mail up to date with the use of recognised security standards? Let us test it through a simple tool.

Related thematic areas:

Culture and skills

Standards

Of particular interest to:

GOVERNMENT

PRIVATE SECTOR

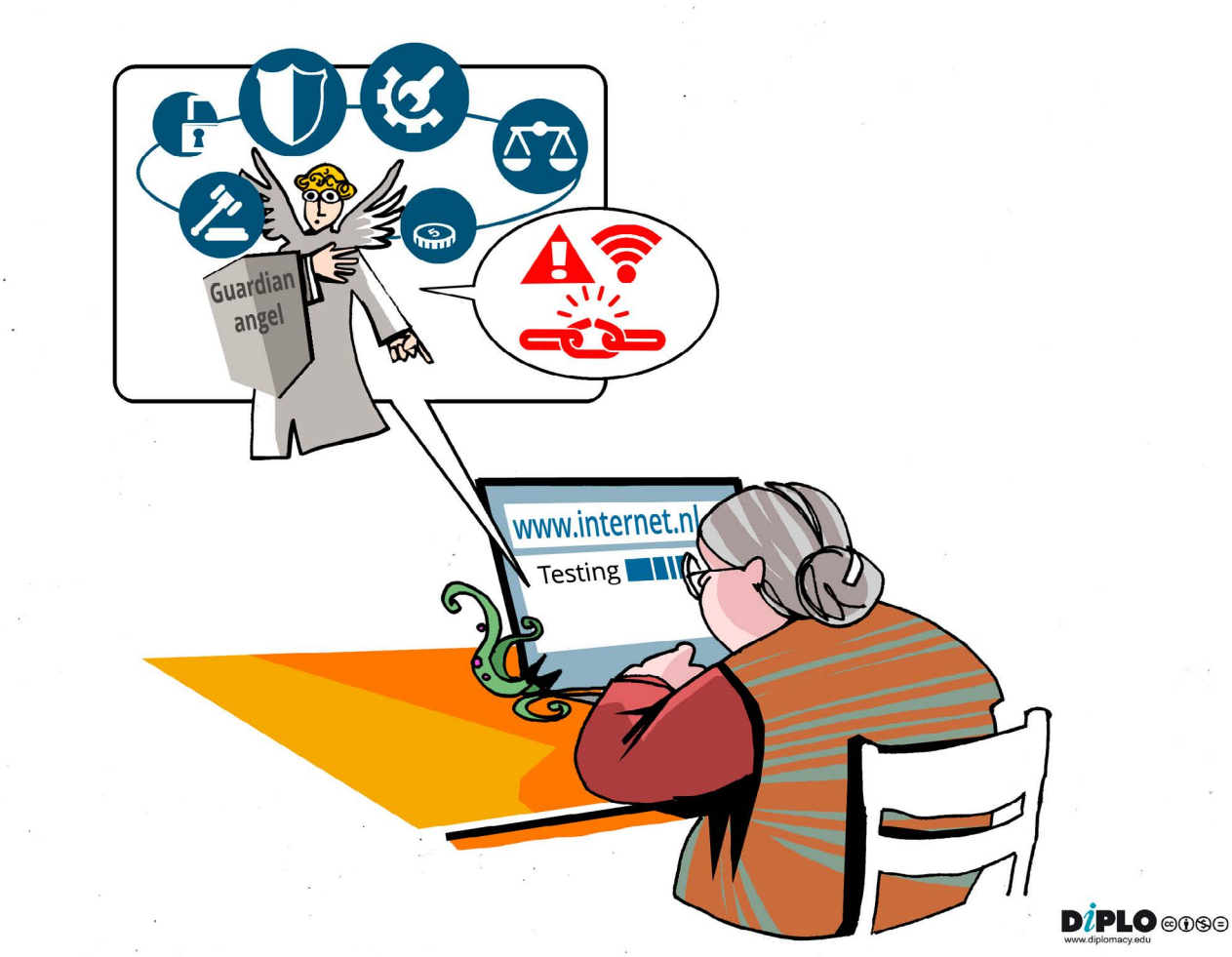
CIVIL SOCIETY

Description

Fully implementing open standards for network services and functions can prevent abuse in various forms (e.g. phishing and botnet infection). Complete and correct standards compliance can diminish the impact of cybercrime and cyber-attacks and lead to more confidence and trust in the Internet, a prerequisite for innovation and fostering an online economy.

To enable and encourage individuals and organisations to use and comply with important standards, free public services for testing compliance with selected standards can be used. An online tool can be set up for the visitor who can – in real time – check any given domain name for security, whether used as a website or within an e-mail address. Users can also test the security of the Internet connection they are currently using when visiting the site. The online tool should provide documentation on the standards supported, as well as a communication channel and point of contact for any national initiative related to the implementation of standards.

While the tool is itself sufficient for technical communities able to identify gaps in standards implementations, the wider community – such as the corporate sector, organisations, and institutions – might need support along with the testing tool. Therefore, a more comprehensive approach involves a platform of organisations that provide support and discuss the implementation of standards (***#MSPlatform***).



Actors (or who this is for)

Targeted stakeholders who implement standards are in general all organisations that rely heavily on the Internet to communicate with users. Typically, these stakeholders are ISPs (access and e-mail), government authorities (e-governance), and the business sector (e-commerce). Yet anyone, including individuals, can use the test tool to check the level of implemented security standards in their own system.
Crucial stakeholders include technical organisations helping with expertise and knowledge, and civil society and governments promoting secure Internet use.

The big picture

The testing tool allows institutions to become more sensitive to respecting existing Internet standards, and thereby increases the overall health of the network.

On a broader scale, it also contributes to partnership building for providing support and coordinating efforts in implementing standards, by creating mechanisms and frameworks for cooperation and collaborative learning. In addition, it contributes at the organisational level by establishing more efficient processes and procedures for improving cybersecurity, especially integration into workflows.

The tool impacts capacity building in several ways:
- Encouraging mechanisms for cooperation on awareness-raising.
- Facilitating expert support and advice.
- Providing input for possible guidelines and good practices.
- Promoting technical standards and encouraging deployment.

Clear analysis of the test results includes easy suggestions for next steps, such as advice to contact your Internet provider to enable IPv6, etc. Complicated technical features are presented in an accessible format. As a result, a simple and intuitive online tool enables a wider circle of users to act independently, which is an important capacity.

Instructions

- Register a simple domain that people can remember.
- Prepare instructions in simple, non-technical language.
- Create a communication platform to promote your tool (***#MSPlatform***).
- Create a support team that will answer users' questions.
- Tailor the components of the web to your national context.

Adaptation to national/regional needs can be arranged based on the existing tool. Different implementations can be envisaged, from simply adding a different language version, to designing a new variant under a different domain, depending on arrangements for the use of source code.

Some possible challenges in replication of this practice include:

- Lack of awareness, which could be mitigated through awareness-raising campaigns (using simple terminology, potentially showcasing metrics).
- Language barriers, which may be addressed through the translation of materials and developing local content.

Timing

Development of a website and a testing tool can run in parallel with setting up a platform (***#MSPlatform***), provided there is a small group of initiators/first movers willing to invest in or put effort to it. The advantage is that the platform, once established, can be operational immediately.

Building a website or tool will take at least a few months (in the case of a straightforward duplicated/translated version of existing practices); while it could take from six to twelve months (if specific needs and adaptations are required).

The lifetime/goals of the platform determine how, and how long, the tools are used. Regardless of how the tools are developed, there will be a continuous need for improvement and further development during their lifetime. New versions should be anticipated as a consequence of testing improvement, new functions, user feedback, bugs, etc.

Example

The GFCE Internet Infrastructure Initiative promotes an up-to-date, open, secure, and future-proof Internet by helping stakeholders to implement open standards for secure e-mail and websurfing, and expanding the Internet address space.

The testing tool made available for the GFCE Internet Infrastructure Initiative, available at www.internet.nl, contributes to the implementation of standards through a variety of uses and mechanisms, for example stick, carrot, exposure, transparency, peer pressure:

- For technicians to improve their employer's ICT.
- For government to generate metrics on the development of security in their agencies and act on it.
- For the press to expose vulnerabilities, sometimes with political impact (the Dutch Minister of the Interior promised to fix the poor security of municipal e-mail across the country).
- For umbrella organisations to test their members.
- For best performing users to be named (hall of fame with 100% score).

The website/test tool www.internet.nl is available in English, Dutch, and Polish and can be used in any country, for any domain, and any Internet connection. Its universality makes it instantly suitable for any national/regional use.

Statistics on the use of the testing tool indicate an increasing trend, while all requests for support, expressed via e-mail to the Dutch community behind this testing tool, were successfully resolved with the parties likely implementing necessary security standards. The tool revealed a lack of security standards in some municipalities, and in response the Minister in charge promised to increase the adoption of standards. Other institutions and communities, such as APNIC, are moving towards implementing the testing tool and web platform.

Source, support, and mentoring

Internet Infrastructure Initiative at the GFCE website: https://www.thegfce.com/initiatives/i/internet-infrastructure-initiative

Internet testing tool: https://www.internet.nl/

Contact point:
Thomas de Haan (T.S.M.dehaan@minez.nl)

Practice: **Establish a clearinghouse for gathering systemic risk conditions data in global networks**

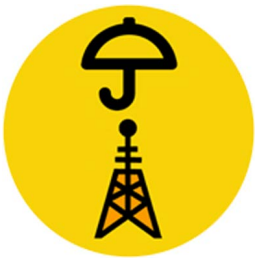
#Clearinghouse

We assess our personal health based on the trusted data we receive from doctors. Cybersecurity is like public health: if CERTs and operators have trusted data — regularly updated — about weaknesses in our networks, this helps them mitigate vulnerabilities, preserve cyber-health, and prevent incidents.

Related thematic areas:

Research and development

Cooperation and community building



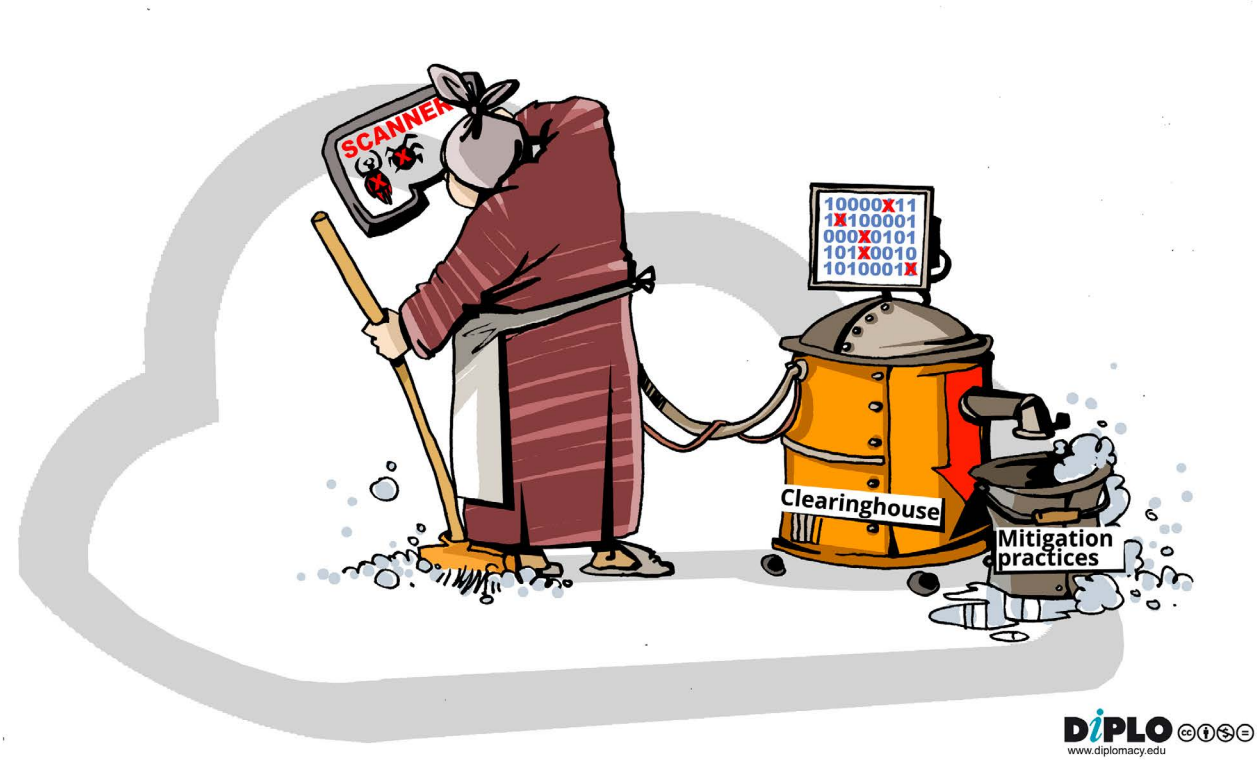
Incident management and infrastructure protection

Of particular interest to:

Description

Internet networks are replete with systemic vulnerabilities. CERTs and other trusted operators require reliable information about their network's health over time. Various organisations have set up systems to scan networks for vulnerabilities and/or monitor cyber-attacks. Many of these sources are open, but their provenance and collection processes are often opaque. To acquire a truly satisfactory picture of the Internet's behaviour, a clearinghouse is needed that does not simply collect data, but leverages its collections to improve the process.

The clearinghouse collects raw data from multiple sources and processes it, in order to feed into Internet health metrics. Data is collected from carefully selected comprehensive data sources, and processed to ensure it is accurate and extensive, and its biases understood and addressed. It can then be analysed and contextualised to produce reliable metrics about how healthy the Internet is.



Actors (or who this is for)

The clearinghouse produces quality data sources that can be used by CERTs, top-level ISPs, and national infrastructure organisations, as well as skilled technical departments within companies or organisations, and regulators to track the health of the ecosystem and suggest improvements. It also allows them to use the clearinghouse's aggregated data along with local proprietary data to generate their own statistics to measure and track the ecosystem's health.

Researchers from multiple communities — academia, CERTs, and industry — are also involved. They can both benefit from the quality data sources for their research work,

and contribute to improving transparent and open algorithms, encouraging scientists to work with and on them. Not least, they can offer additional sources of data to the clearinghouse.

The big picture

The tactics used in cyber-attacks change constantly, but the overall process and goals vary less. For instance, a DDoS attack can be conducted using a botnet, a collection of script kiddies, or through a reflection attack using misconfigured servers on the Internet. However, they all represent minor variations of the same basic approach — flooding connections with garbage data in order to stop a target from communicating. Most solutions are oriented either towards investigating each new variant of threat that emerges separately, or blacklisting some corrupted servers.

It is the root of the problem that should be addressed, however, because the root cause of attacks are vulnerabilities, both in the implementation and the specification of software. These vulnerabilities constantly change as new problems are discovered. It is impossible to simply patch ourselves into safety. Instead, CERTs, operators, and policymakers must address this as a problem of triage – what are the most impactful problems, and what are the most effective mechanisms to mitigate that impact? While there are numerous sources of information about vulnerabilities across the Internet, this data should be carefully selected, compiled, and synthesised in order to construct a reliable and trusted transparent image of the health of the Internet and its segments.

The clearinghouse establishes accurate and comprehensive data sources through continuously seeking to identify, recruit, and process the best possible globally available data sources to service the measurement of global cyber health and risk conditions. These sources should evolve as the understanding of cyber health improves and measurement advances. Being processed to raise transparency and comparability of data between various actors, they serve as a trusted base for mitigation.

The technical community, and particularly CERTs and operators of Autonomous Systems, acquires a tool that increases their capacity to identify risk conditions. If the clearinghouse 'engine' is open source, the knowledge of how to validate and process raw data to make it actionable and support effective decision-making can be improved.

Instructions

The clearinghouse develops and maintains quality data sets related to risk indicators. It should collect and process data.

Collecting data

Data should be collected from existing sources (academic and research projects, corporate initiatives) and from own network scanning.

Data collection methods must be transparent (which is not always the case with commercial sources). Elements for measuring the quality of the collected data should be developed and made public.

While network scanning can bring additional quality information, it is also a risky approach: if too many players are involved, it can make a network a very noisy environment. In addition, since scanning is done by the perpetrators as well, the scan targets may block the traffic if they start receiving too many scans. Several legitimate organisations involved in scanning networks already exist — though without much coordination; so, it may be better to use their results, or at least coordinate efforts with them.

Processing data

Processing the collected raw data may include
- Cleaning
- Matching
- De-biasing
- De-duplicating

Network security data, such as scan results, are highly time-sensitive. There is an enormous amount of transient activity on the Internet, and it is reasonable to believe that some fraction of true positives from scan results are invalid within hours of the scan's completion. Because of this, pure IP address information provides an illusion of precision.

Cleaning ensures a focus on relevant data. Matching ensures a more complete picture, as various sources report on different parts of the Internet at different times. De-biasing considers the fact that most commercial sources are biased in some way. De-duplicating removes duplicated data.

It is important that data processing and statistical engines be open source and available for free to security operations teams, so that others can replicate the platform, analyse, and develop statistics with their own sources, and contribute with possible improvements to the engine.

Timing

The timeline vastly depends on technical and operational capabilities and specific needs. A provisional timeline for developing a clearinghouse may be as follows:

Collecting data

Data, especially OSINT sharing is based on trust derived from security operations and collaboration. It might take some time to build trust, if the organisation is not in the trusted operations community already. This can take between six months and a year.

Processing data

The organisation needs to hire really good data scientists, who also have a cybersecurity background. These people are rare, and it is hard to recruit them, so establishing a team may take six months or more.

Example

The GFCE initiative CyberGreen makes the cyber-ecosystem healthier through measuring and visualising the state of the global cyber ecosystem, and producing materials for mitigating negative impacts. The clearinghouse is one of the main achievements of the initiative, along with metrics and visualisations, and support for mitigation.

CyberGreen works with data scientists and statisticians from multiple national CERTs as well as private industry. CyberGreen also works with Regional Internet Registries - RIRs (APNIC, LACNIC, RIPE, etc.), Regional CERTs (APCERT, TF-CSIRT, Africa-CERT, ITU-ARCC) for mitigation training and capacity building.

CyberGreen's current sponsors include JPCERT/CC, the Cyber Security Agency of Singapore, and the UK Foreign and Commonwealth Office. These and other policymakers benefit from having increased visibility of the risk levels that are present in their countries.

Source, support, and mentoring

CyberGreen statistics site: http://stats.cybergreen.net
Data sources catalogue by CyberGreen: http://www.cybergreen.net/data-inventory/
Bulk data (and API) of CyberGreen for download: http://stats.cybergreen.net/download/

Contact CyberGreen:
https://www.cybergreen.net/contact/

Contact point:
Yurie Ito (yito@cybergreen.net)

Practice: **Produce and present trusted metrics about systemic risk conditions**

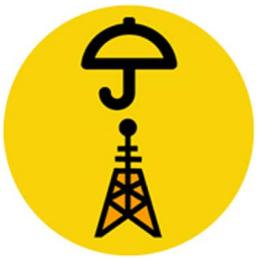
#HealthMetrics

All those figures on a medical test report do not mean much to us — we need a doctor to analyse various data, contextualise it for our body and lifestyle, and present us with the findings in a comprehensive way. The same goes for network health — trusted data needs to be turned into vetted and well-presented metrics, to increase awareness and incentivise action by responsible companies, organisations, and institutions.

Related thematic areas:

Research and development

Cooperation and community building



Incident management and infrastructure protection

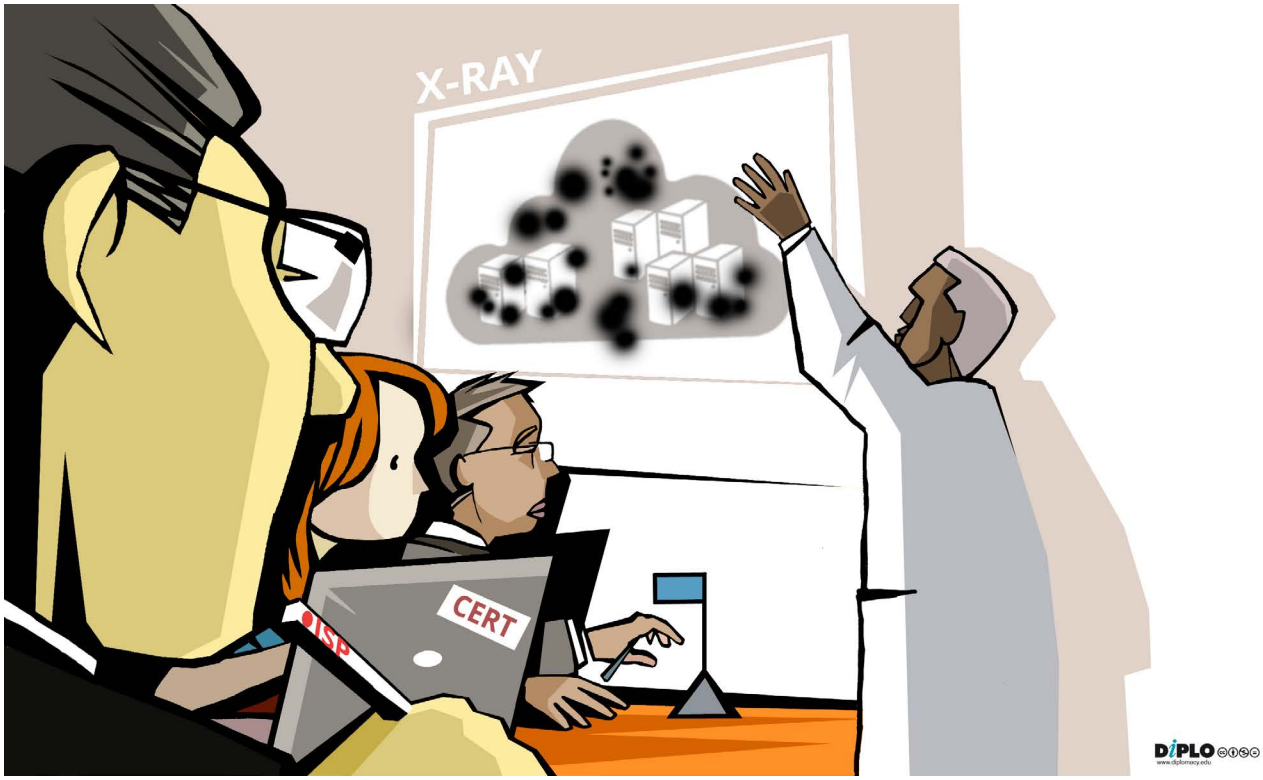
Culture and skills

Of particular interest to:

Description

Statistically mature and vetted metrics, rather than raw data, should be presented to the parties in charge of keeping the network clean. The development and application of statistical methods to data allows for measurement and contextualisation of key indicators of malicious activity and risk conditions. Metrics should be normalised transparently, so that users can interpret and use the data in their own way.

A statistics platform, featuring metrics and data visualisation, allows for the measurement of key indicators of malicious activity and risk conditions, and enables analytical insight about patterns, priorities, and trends for action. Such intelligence can be used by the CERT/CSIRT community, security sector, corporations, and organisations. If the metrics are regularly published in reports about the health of the cyber-ecosystem and the mitigation impact, the decision-making level — including CEOs and government ministers — could become more aware and ready to act.



Actors (or who this is for)

Everyone can benefit from obtaining trusted, clear, comprehensible data about the health of cyberspace:

- CERTs can use it to enhance the trust of their partners, to prepare situational awareness, and to issue early warnings.
- Network operators are expected to monitor the conditions of their networks and act accordingly. Clear metrics can assist them in identifying risks and trends.
- Security departments in companies, institutions, and organisations can likewise benefit from receiving clear metrics on trends in their environment.

- Governments can improve policy and operational responses to risks, if they are regularly informed about the health of the national network and the environment.
- Academics and researchers can use metrics to pursue additional research work.

In addition, several stakeholders can contribute to improving metrics. CERTs and network operators can feed into the metrics with particular data sets, as well as with information about the specific local use of the Internet and its services. If metrics methods are transparent, academics and researchers can validate them and help with improvements, and experts can replicate them for different purposes.

The big picture

The prevention of cyber-incidents is primarily based on a healthy cyberspace. On the operational level, CERTs can point to critical risks, while operators should mitigate flaws in their networks. On a policy level, policymakers should decide on strategic steps and action plans. All of them would benefit from trusted and processed intelligence about the health of the network presented in formats comprehensible to them.

Existing cybersecurity practice focuses on minimally processed data, commonly present in raw format which is useless to anyone but a particular niche of technical operators. Higher quality and more actionable data should be turned into metrics, through the analysis of carefully selected and processed comprehensive data sources and visualised presentations.

Using such metrics for regular monitoring of the health of the networks can assist CERTs in communicating with partners and provide them with a trusted picture of the condition of their networks. Operators and companies, organisations, and institutions in general can enhance their skills for understanding risks, thanks to clear risk indicators provided by the metrics. The metrics can increase the capacity of the decision-making level in corporations to assess risks and provide resources for mitigation. Similarly, they can improve awareness among policymakers and state decision-makers about cyber-risks, and enable them to more clearly recognise what policy approaches could help mitigation. Not least, thanks to the visualised and comprehensible metrics — possibly presented to the wider audience through CERTs — end-users can become more aware of the security risks and increase their demand for a cleaner network and safer cyberspace.

In addition, the continuous measurement of network health can lead to noticing improvements and identifying mitigating factors, which may allow the extension of lessons learned and good practices in mitigation.

Instructions

Metrics should be based on trusted, comprehensive, and pre-processed data sources, such as those developed through the clearinghouse approach (***#Clearinghouse***).
To make it action-oriented, metrics need to be based on the statistical analysis of raw data.

If possible, data should also be normalised for local Internet conditions or network usage. For instance, the majority of scanning and analyses have been conducted in the IPv4 space, yet with the increasing use of IPv6, it is necessary to consider the implications of IPv6's massive address allocation and its impact on normalising results across groups of addresses. Also, bandwidth consumption and usage differ significantly between different regions. For example, even minor habits, such as the tendency for American computer users to leave their systems on all the time, can affect propagation and botnet impact. Normalisation should be done at the level of the metrics, and with transparent methods so that users can understand how it is done. It also allows comparability and eliminates the need to interpret the data on the client's side. Local partners, such as ISPs and CERTs, can help with understanding local factors and feed them into the normalisation methods.

The metrics should be presented in an accessible and transparent format, with regular updates. For instance, an online platform could feature metrics searchable by country or geographical region, by network (e.g. Autonomous System Numbers), and by risk. Visuals, such as maps and graphs, are of particular relevance for easier understanding by various stakeholders.

Of particular relevance for outreach to decision-makers and CEO-level professionals is publishing regular (e.g. biannual) analysis reports featuring trends, risks, and mitigation impacts. Such reports should be accompanied by materials for policymakers about how to understand the metrics — what they show, and what mitigation approaches are possible. This can be linked with the production of training materials for various stakeholders.

There are several challenges to take into consideration. It is essential to build trust among other possible partners that should contribute to and use the metrics, which takes time. Processed data may not lead to actions by operators if they are not correlated with actionable steps a provider can take. When it comes to the presentation of metrics, it is very important that it does not include naming and blaming, as this would reduce trust and the readiness of third parties to act accordingly. The metrics are there to monitor the health of the network, and to incentivise parties to contribute to the mitigation of identified risks.

On a more general level, measuring network conditions is not the only possible measurement, and it does not necessarily reflect comprehensively the actual state of security for a particular environment. It may therefore be important to seek links with other initiatives that implement different measurements, such as the number of vulnerabilities within a product, or the use of penetration testing, to compile a more comprehensive view.

Timing

The timeline vastly depends on technical and operational capabilities and specific needs. Developing trusted metrics that can also be useful and easily readable by a variety of actors requires at least a year, with ongoing improvements.

Example

The GFCE initiative CyberGreen makes the cyber-ecosystem healthier through measuring, visualising, and mitigating negative impacts. Its Statistics platform v.2 features metrics-based measurement and visualisations as well as the ability to compare across countries and autonomous systems.

Several partners are using CyberGreen metrics for decision-making and additional research. Singapore uses the metrics to move policymakers to act. The Singapore ICT Minister has presented the results to other ICT ministers in the ASEAN region and encouraged them to use the platform and metrics to facilitate national and regional mitigation campaigns, while CyberGreen assisted with establishing a regional platform to follow the health statistics of each country in the region, and provide capacity building materials. Japan is also encouraging partners in Asia-Pacific and other intergovernmental forums to start using it, while ITU-ARCC is using CyberGreen metrics and training materials to encourage its members to act.

The biannual report published by CyberGreen has been used by many stakeholders, and has been presented at ministerial level (such as at G7 and G20) for several years to raise awareness among decision-makers.

CyberGreen's current sponsors include JPCERT/CC, the Singapore CSA, and the UK FCO. These, and other policymakers, benefit from having increased visibility of the risk levels that are present in their countries.

Source, support, and mentoring

CyberGreen Statistics platform:
http://stats.cybergreen.net/

Contact CyberGreen:
https://www.cybergreen.net/contact/

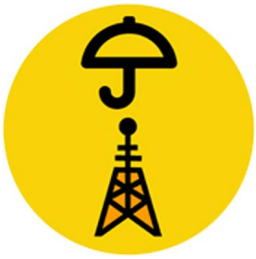
Contact point:
Yurie Ito (yito@cybergreen.net)

Practice: **Assist with cyber-risk mitigation and keep score of successes**

#Scorekeeping

Weight loss does not happen by learning theory, but by practical exercises — and certainly by keeping records of successful steps. Similarly, network operators need help with monitoring the systemic risks, providing training materials and practical experience for mitigation, but also keeping track of successful actions.

Related thematic areas:



Incident management and infrastructure protection

Culture and skills

Cooperation and community building

Of particular interest to:

Description

To prevent cyber-incidents, root cause systemic risks should be addressed rather than symptoms. However, understanding, identifying, and mitigating the systemic risks are not easy. Complete, reliable, and well-presented metrics that identify risks in particular networks need to be coupled with assistance for mitigation and continuous monitoring of the health of the network to evaluate success.

Training materials built on mitigation practices in the context of particular risks addressed can teach ISPs, as well as other organisations and policymakers, what is needed to mitigate particular vulnerabilities. **Capacity building support** developed around these materials, mitigation practices, and risks can increase the efficiency of mitigation.

Scorekeeping success through continuous measurement of the health of the network identifies improvements and mitigation efforts by various parties. It also identifies new risks, and incentivises partners to act collaboratively rather than competitively. Scorekeeping can also extend the collection of good practice for mitigation.

Actors (or who this is for)

Network operators, ISPs, and vendors bear the major responsibility for improving the health of networks. They are, therefore, the main beneficiaries of any capacity building programme and scorekeeping, which should incentivise and enable them to mitigate risks.

RIRs and CERTs communities which already provide capacity building and support to operators and policymakers, as well as capacity building institutions providing support in cybersecurity, can integrate training materials into their work.

Policymakers are also a particularly important stakeholder group, since their greater awareness about risks in the networks within their geographical area, mitigation efforts, and responsibilities of key players, may lead to better policies — both incentives and regulations — to ensure a healthier network.

The big picture

While CERTs warn about risks and assist partners with mitigation, it is the partners that must act in response to alerts. Few network operators and vendors can manage to address root causes, as there are always immediate threats facing these organisations that divert attention from analysing root causes.

Most ISPs and vendors could better apply knowledge to identify common root causes if assisted to track, identify, and understand risks in each network and at each moment, provided with training materials and capacity building for mitigation, and if score is kept about successful mitigation to commend proactive actors and share additional good practices.

Policymakers should, however, also benefit from capacity building. While they might not need to understand the details about mitigation practices, the metrics (*#HealthMetrics*), scorekeeping, and understanding the risks and responsibilities of major players, can assist them to develop a suitable policy environment to incentivise — or demand — operators and vendors to implement mitigation practices.

Instructions

Training materials are developed based on good mitigation practices, coupled with metrics pointing to specific risks for particular networks. Good practices can also be identified thanks to scorekeeping: Since the impact of mitigation efforts show up clearly in the metrics, it is possible to find which Internet service providers did the mitigation work and to record and share their practices.

Scorekeeping represents measuring the health of the network at different points in time. It is conducted by charting the improvements in metrics using timelines. Mitigation efficacy analysis is performed based on the timeline trend analysis, along with identifying the high-impact root-cause mitigation practices, and then sharing the practices with partners through training and capacity building to make them easy to replicate.

Capacity building activities should ensure the implementation of good mitigation practices. It is suggested to integrate mitigation training materials into various existing capacity building programmes through partnerships with capacity building institutions, so that a diversity of stakeholders can be targeted.

For mitigation to actually happen (e.g. re-configuring servers or replacing outdated devices), additional market incentives and regulation might be needed. These efforts can impact the governance model, as well as the market cycle; for instance, supporting vendors in examining cyber-hygiene and empowering users to demand security can in turn improve the vendor's return in the long term.

Timing

Developing a collaboration channel with capacity building institutions may take about two months. Developing trust building with data sources may take another one to two months. Preparing the training and workshop materials and delivery on mitigation techniques may take another one to two months. The materials and delivery should continuously be updated based on the data gathered for scorekeeping.

Example

The GFCE initiative CyberGreen makes the cyber-ecosystem healthier through measuring, visualising, and mitigating negative impacts. The initiative has built a library of training material, and offers assistance with training to various partners.

CyberGreen works with RIRs (APNIC, LACNIC, RIPE, etc.) and Regional CERTs (APCERT, TF-CSIRT, Africa-CERT, ITU-ARCC) in mitigation training and capacity building. The ITU uses CyberGreen metrics and training materials to encourage its members to act. Other partners (e.g. APCERT, ITU-ARCC, Africa-CERT) reference CyberGreen training materials to use for their own training. Countries in the ASEAN region, with the support of Singapore and CyberGreen, have established a regional platform to follow the health statistics of each country in the region, and to provide capacity building materials.

CyberGreen's current sponsors include JPCERT/CC, the Singapore CSA, and the UK FCO. These and other policymakers benefit from having increased visibility of the risk levels present in their countries.

Source, support, and mentoring

CyberGreen training materials: http://www.cybergreen.net/mitigation/#capacity-building-materials
Various related presentations: https://www.cybergreen.net/blog/?category=presentation

Contact CyberGreen:
https://www.cybergreen.net/contact/

Contact point:
Yurie Ito (yito@cybergreen.net)

Practice: **Align national campaigns**

#Campaign

Your awareness campaign is probably not the only one – other campaigns are taking place locally, nationally and/or internationally. It is advisable to align them to have greater impact and use resources more efficiently. Aligning campaigns supports the ultimate goal of raising awareness of cyber-threats through safe online behaviour.

Related thematic areas:

Cooperation and community building

Cybercrime

Culture and skills

Of particular interest to:

Description

Cooperation, alignment, and coordination with others is beneficial. In planning and organising an awareness campaign, it is advisable to coordinate with other existing national and international awareness campaigns. If stakeholders come together to share materials, and possibly align messages, the impact is amplified. **Sharing materials and aligning campaign messages helps to broaden the impact beyond one constituent community.**

With cooperation and alignment, stakeholders can easily see what others have already done, learn from their mistakes, and consider these experiences as models. Moreover, they can leverage different components from one another. A coherent, coordinated multistakeholder campaign is an efficient use of limited resources, and will become more effective in its goals, for example in empowering citizens to adopt safer and more secure practices online.

Actors (or who this is for)

International and national partners in government, academic, non-profit, and private sectors, who are a part of, or seek to create a national-level awareness campaigns.

The multistakeholder approach is promoted, as the supply chain of the Internet involves various actors who have varying levels of responsibility and the ability to make positive impacts.

The big picture

The exchange of experience can support capacity building both for more experienced partners, who get to reflect on their practices and learn through sharing, and for less experienced partners who could avoid unnecessary mistakes and move more quickly towards effective practice. Of course, practices will always need to be adapted to the local environment.

Organisational capacity is strengthened by assisting partners to work more effectively together, and ultimately, through the campaign, the end-users benefits from increased capacity on how to use the Internet safely.

Instructions

- Gather stakeholders for dialogue and make efforts to coordinate events and activities. Align the vision, messages, and themes of the campaign among partners.
- Ensure that there is a shared vision.
- While the substance and information are the same for all, make sure to conceptualise campaigns for a specific constituent base. Often, it cannot be just copied and pasted.
- Cooperate and align with stakeholders on a variety of levels: domestically across stakeholder communities, bilaterally and/or regionally, and internationally.

- Coordinate cyber-focused events both in person or via social media while promoting the concept of multistakeholder involvement in the implementation of national awareness-raising initiatives.
- Work on sharing materials and toolkits, and proactively promote existing available resources. Reuse existing materials to reduce the cost of campaigns and to avoid reinventing the wheel. In this way, contextualised and repurposed materials can be used for other domestic and/or international campaigns. This also contributes to lower costs.
- Consider sharing the materials for free.
- Prepare a partner package with basic instructions, and point your partner to available resources. Direct partners to specific sections rather than sharing overwhelming amounts of information with them.
- Try to tailor the partner resources to the region (for instance, in Africa, mobile phones are very popular – tailor the format of your resources accordingly).
- Fit your message and campaign style to the context of the message. Be prepared for the fact that other partners may want to share their message in a different way.
- Consider local specificities, including the culture of the organisation you are working with.
- Utilise existing sharing platforms, for example the Stop.Think.Connect.™ Cyber Awareness Coalition.
- Measure your campaign in terms of reported successes and participation.

It is important to be aware of obstacles, such as the language of the campaign. Other obstacles are trademarks and copyrights which can be a challenge when looking to repurpose and contextualise other organisations' material.

Timing

Timing is dependent on the implementation time of the campaign. Sufficient time needs to be given for coordination, in the framework of ten months for a major campaign (***#Month***); otherwise campaigns are on-going coordinated efforts.

For smaller-scale campaigns, an agile approach is recommended, enabling a quick and flexible reaction to new developments or incidents.

When approaching partners, take into consideration the time of the year to avoid major celebrations, holidays, or vacation periods.

Examples

The GFCE's Global Campaign to Raise Cybersecurity Awareness Initiative raises awareness of cyber-related threats and good practices worldwide, empowering citizens with the knowledge and a sense of shared responsibility to practice safe and informed behaviour on the Internet. By leveraging expertise from international partners in government, academic, non-profit, and private sectors, this cybersecurity awareness campaign initiative works broadly with stakeholders to ensure a safer and more secure Internet for all.
GFCE members pursue opportunities for collaboration on raising cybersecurity

awareness around the globe, including fostering cooperation and alignment where possible between Stop.Think.Connect.™ and existing cybersecurity awareness campaigns in other countries, joint promotion of cyber safety resources, and good practices. The Initiative provides a partner package with basic instructions for partners implementing awareness campaigns on similar topics, with a set of resources as used in the Global Campaign to Raise Cybersecurity Awareness.

Source, support, and mentoring

More information on the GFCE's Global Campaign to Raise Cybersecurity Awareness:
https://www.thegfce.com/initiatives/g/global-campaign-to-raise-cybersecurity-awareness

Contact point:
Joanna MC LaHaie (LaHaieJMC@state.gov)

Practice: **Focus awareness-building through a cybersecurity Awareness Month**

#Month

Declaring a month dedicated to cybersecurity awareness can help focus the efforts of many stakeholders and enhance their collaboration, while delivering a strong message to the public, and increasing the effectiveness of capacity building efforts.

Related thematic areas:

Cooperation and community building

Culture and skills

Of particular interest to:

Description

The National Cybersecurity Awareness Month (NCSAM) is an example of a cybersecurity awareness campaign at national level that builds on the attention provided by declaring a month dedicated to a specific topic to mobilise actors; raise the activity profile; and amplify communication, awareness, and capacity building activities.

The campaign focuses on different topics each year. Each week of the one-month campaign is dedicated to a particular topic, which can vary from awareness building, to practical skills, behaviour, and tools for end-users.

One of the important features of the campaign is a **call to organisations and individuals to become its champions**. Another important feature of the **campaign are the very practical suggestions of how to get involved and contribute**. This includes concrete things to do on social media, at home in the family setting, at school, and at work (e.g. organising a 'brown bag' seminar).

While NCSAM stands on its own as a global good practice, to be supported and adopted by those who are still not promoting it, it is also a pattern for more general practice – that of an awareness month (or week), dedicated to a different topic, where there is a need to provide focus for awareness building on a large scale.

Actors (or who this is for)

National governments, through their bodies in charge of cybersecurity awareness, are the most effective owners of this type of campaign, as they can reach out and mobilise all the other national actors (technical community, academia, business, etc.). However, in cases where this is not possible, other influential national-level actors, such as large universities could also take the leading role in establishing and promoting a national awareness month.

Other stakeholders participating in the campaign have an equally important role. Without their active participation in distributing information and resources and facilitating events, the campaign would have little effect. The campaign should aim to include the business sector, academia, the technical community, and citizens in general.

The big picture

From the capacity building perspective, an awareness-raising campaign such as this practice, contributes first towards engaging stakeholders and sharing a vision, then towards learning and improving the various capacities of the broadest constituency – in this case citizen end-users.

Depending on the available resources and commitment of organisers and partners, an awareness-oriented month can provide many opportunities for learning, including training for concrete competencies and practical skills. It can also be used to provide tools and resources, and thus contribute towards a safer and more effective use of the Internet, related technologies, and applications.

With sufficient international adoption, campaigns of this nature can also promote international cooperation around the targeted topic, and strengthen the widest systemic capacity for the safe use of digital tools and media.

Instructions

- Gather the highest possible level (governmental) support and commitment for the campaign, inspire partners, and share the vision.
- Continuously monitor topics of interest for the campaign in question and identify themes and topics that are most likely to be of relevance for the upcoming campaign, in a timely manner.
- Create communications material around the selected topics, appropriate for partners and end-user audiences.
- Publish calls for partnership, encouraging diverse stakeholders to take part in the campaign.
- Ensure that communications explain concrete and achievable ways to participate, for all stakeholders.
- Use social and traditional media, and face-to-face events to communicate and promote the campaign and its activities.

Timing

A possible timeline:
- D-10 months: Careful monitoring of themes and topics
- D-6 months: Selection of themes and topics covered
- D-6 to -3 months: Work on communications material
- D-3 to -1 month: Distribution of materials and final preparations

Examples

The GFCE's Global Campaign to Raise Cybersecurity Awareness Initiative raises awareness of cyber-related threats and good practices worldwide and empowers citizens with the knowledge and a sense of shared responsibility to practice safe and informed behaviour on the Internet. By leveraging expertise from international partners in the government, academic, non-profit, and private sectors, this cybersecurity awareness campaign initiative works broadly with stakeholders to ensure a safer and more secure Internet for all. The initiative encourages global adoption of October as NCSAM.

Cybersecurity Month:

NCSAM, October, https://staysafeonline.org/ncsam/
ECSM, October, https://cybersecuritymonth.eu/

Other global awareness campaigns:

UN World Cancer Day, 4 February, http://www.un.org/en/events/cancerday/
UN International Disarmament Week, 24–30 October, http://www.un.org/en/events/disarmamentweek/

Source, support, and mentoring

More information on the GFCE's Global Campaign to Raise Cybersecurity Awareness: https://www.thegfce.com/initiatives/g/global-campaign-to-raise-cybersecurity-awareness

Contact point:
Joanna MC LaHaie (LaHaieJMC@state.gov)

Practice: **Stimulate local ownership of capacity building programmes through National Project Teams**

#NationalTeams

How can international and regional forums, donors, and development agencies stimulate local ownership of the capacity building programmes they wish to support? How can countries ensure commitment in capacity building efforts?

Related thematic areas:

Cybercrime

Culture and skills

Of particular interest to:

Description

To achieve local commitment and ownership, the global actor – a donor, an aid agency, or an international organisation – offering support and resources for a particular capacity building initiative should engage in a dialogue with the government about participation in this initiative. If the government wishes to participate, it should be requested to establish a **National Project Team** which is to be composed of officials meeting a defined set of criteria or representing specific ministries or other institutions.

The National Project Team plays a crucial role in implementing capacity building activities at the national level. Members are required to mobilise their respective institution, to contribute to the project work plan, to support the organisation of activities, to mobilise participants in activities, etc.

The composition of the National Team is thus essential. Officials selected for the team should have sufficient decision-making power, but not be too highly placed in order to reduce potential political pressure. In addition, one member is to function as National Coordinator.

In this way, a project can involve multiple institutions within a country, ensure local ownership, facilitate inter-agency cooperation, and avoid cumbersome administrative procedures each time an activity is organised.

Actors (or who this is for)

- International, regional, and bi-lateral organisations, donors, and other national and international stakeholders offering resources and support for capacity building in the cyber sphere.
- Government ministries, national bodies, law enforcement authorities, and training institutions interested in strengthening national cyber capacities.

The big picture

One of the essential recommendations for the success of capacity building programmes is that they should be 'owned' by the people and organisations benefiting from them. Without local ownership and engagement, capacity building programmes are considered 'external assistance', with many risks, downsides, and inefficiencies that were observed during the past decades of international development cooperation, based on the traditional assistance model.

However, important resources for capacity building programmes are mostly available externally – within global networks, international forums, or organisations. This is particularly the case in the cybersecurity sphere, where international forums have a major interest in improving the capacity of individual states in order to strengthen the global network and render it a safer environment. Facilitating local ownership and commitment for programmes that are designed and resourced 'elsewhere' is not an easy task due to inherent tensions.

Instead of imposing the engagement of national beneficiaries, international partners should encourage and stimulate local commitment and ownership. They first need to target specific regions or countries to work on raising awareness of the challenges that could be addressed, and the capacity building programmes and resources required and available. Once the awareness and the needs are expressed, the commitment towards a joint programme may be stronger.

Instructions

Preparatory phase

- Raise awareness of the challenges and needs in countries.
- Raise awareness of available capacity building programmes.
- Match local needs and global offers.
- Obtain government commitment to participate in a particular programme.
- Request the government to appoint a National Project Team based on a set list of criteria (i.e., represents key counterpart institutions).

Implementation phase

- Upon formal response from the government, involve the National Project Team in a detailed initial assessment of the situation. This is to result in a situation report representing the baseline against which progress can be assessed at a later stage.
- Assist the National Project Team in the preparation of a project workplan.
- Make members of the Team responsible for the organisation of activities with the support of the project.
- Involve the Coordinator and the Team in Project Steering Committee meetings.
- Involve the National Project Team in monitoring and evaluation exercises to determine progress made.

Timing

The time required for the process described varies greatly, because the preparatory phase may be very different from one region to another. The regional policy processes, which play an important role, may be at very different stages. Six months to two years is needed for awareness building.

Once a country has requested capacity building assistance, the process of establishing a National Team and starting to engage in capacity building activities may take three to nine months.

Examples

The GFCE Initiative relates to Global Action on Cybercrime Extended (GLACY+) project, a joint project of the Council of Europe and the European Union. It follows the GLACY project from 2013 to 2016.

GLACY+ relies on the lessons learnt, materials developed, and best practices identified from the experience of seven priority countries in Africa and the Asia-Pacific region – Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka, and Tonga – in the strengthening of their criminal justice capacities on cybercrime and electronic evidence and enhancing their abilities for effective international cooperation in this area.

GLACY+ extends this experience by enabling GLACY priority countries to serve as hubs and share their knowledge with other countries in their respective regions. Countries in Latin America and the Caribbean are now also benefitting from project support.

GLACY+ extends its outreach and partnerships through the GFCE. The project provides several examples of countries that have requested capacity building and have formed National Teams.

Source, support, and mentoring

The source for defining this practice is the joint project of the European Union and the Council of Europe – GLACY+.

More information:
- GLACY+ summary: https://rm.coe.int/168063f695
- About GLACY+: http://www.coe.int/en/web/cybercrime/glacyplus
- GFCE Initiative GLACY+: https://www.thegfce.com/initiatives/g/glacy

Contact points:
- Matteo Lucchetti (matteo.lucchetti@coe.int)
- Manuel de Almeida Pereira (manuel.pereira@coe.int)

Practice: **Enhance capacity building outreach through regional hubs**

#RegionalHubs

Capacity building programmes may be hard and costly to implement at multiple locations around the world, especially in distant regions. How can we effectively reach out with capacity building support in a particular region? What if a decentralised model were encouraged, supporting local champions to develop and help others?

Related thematic areas:

Cooperation and community building

Cybercrime

Culture and skills

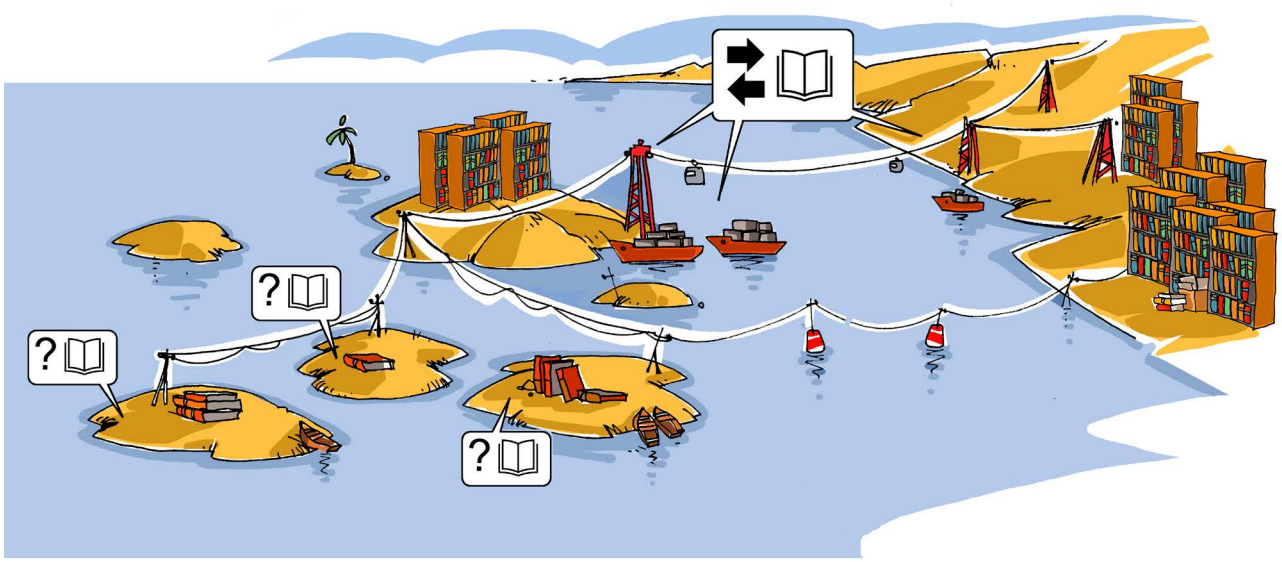
Of particular interest to:

GOVERNMENT

LAW ENFORCEMENT

Description

Countries that have benefitted from capacity building activities previously, that have reached a certain level of maturity, and have experience to share may serve as **regional hubs to share their experience within their respective regions**.



Actors (or who this is for)

- International organisations, donors, and other national, regional, and international stakeholders offering resources and support for capacity building in the cybersphere.
- Government ministries, national bodies, law enforcement authorities, and training institutions in countries that already promote regional cooperation and wish to provide further support, establishing themselves as a reliable partner in a region.

The big picture

Global capacity building initiatives sometimes appear remote, less accessible, and less relevant to actors in a given region, if the initiative is designed and managed from far away. Despite the type of communications channels used today, the lack of immediate contact, cultural differences and scarce information flows can act as inhibitors for full awareness of the availability of support for capacity building.

Establishing capacity in one country of a region, however, could help strengthen capacity in neighbouring countries as well. Having a local hub and a champion in a region can facilitate awareness-raising of the opportunities for accessing a global programme that may appear somewhat distant at first. The support provided through local hubs can also reduce costs and increase responsiveness to the needs of those requesting support and resources for capacity building.

Such an approach can also be a good way to reach out to distant regions, such as the Pacific Islands. In addition, a regional hub can lead to the interest of other neighbouring countries in such a programme, and they may request assistance.

Instructions

- Select a country that could serve as a hub and engage in a dialogue.
- Define the skills and experiences that this country could share within its region and with project support.
- Liaise with other organisations and projects active within the country to seek synergies and avoid duplication of efforts.
- Further strengthen the capacities of the hub country, for example, by supporting the organisation of regional training events.
- Support the chosen partner country in reaching out to other countries in the region to raise awareness about needs, and opportunities offered by the capacity building programme.
- Support the chosen partner country in delivering or co-delivering capacity building support to other countries in the region.

Political and other sensitivities within regions need to be considered when selecting and supporting hubs. Not all countries in a region will be prepared to cooperate. Political changes may also affect the readiness to cooperate.

Timing

Once a hub has been selected, the process can be initiated at any time by organising a regional activity and by using that momentum for follow up.

Examples

The GFCE Initiative relates to Global Action on Cybercrime Extended (GLACY+) project, a joint project of the Council of Europe and the European Union. It follows the GLACY project from 2013 to 2016.

GLACY+ relies on the lessons learnt, materials developed, and best practices identified from the experience of seven priority countries in Africa and the Asia-Pacific region – Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka, and Tonga – in the strengthening of their criminal justice capacities on cybercrime and electronic evidence and enhancing their abilities for effective international cooperation in this area.

Several of these GLACY countries now serve as hubs under GLACY+. In West Africa, ECOWAS has now also become a partner.

Source, support, and mentoring

The source for defining this practice is the joint project of the European Union and the Council of Europe – GLACY+.

More information:
- GLACY+ summary: https://rm.coe.int/168063f695

- About GLACY+: http://www.coe.int/en/web/cybercrime/glacyplus
- GFCE Initiative GLACY+: https://www.thegfce.com/initiatives/g/glacy

Contact points:
- Matteo Lucchetti (matteo.lucchetti@coe.int)
- Manuel de Almeida Pereira (manuel.pereira@coe.int)

Practice: **Assess national cybersecurity capacity using a maturity model**

#MaturityModel

Capacity building is most effective when it builds on existing capacities. How can we have a better picture of current capacities and capabilities? Assessing national cybersecurity capability and readiness using a maturity model provides a comprehensive review of existing capacities which can be further developed, and offers recommendations for setting priorities.

Related thematic areas:

Policy and strategy

Culture and skills

Standards

Cooperation and community building

Of particular interest to:

Description

As countries turn to planning their strategic cybersecurity steps, it is of the utmost importance to assess their existing capacities and capabilities. Using a cybersecurity **maturity model** allows governments to do a comprehensive review of a country's cybersecurity capacity, where it stands, what the gaps are and what concretely could be done to improve, and how to build capacity. Based on the results, policymakers and other stakeholders are able to set priorities for capacity building and investment.

Actors (or who this is for)

- Governments, and in particular, their agencies responsible for cybersecurity, or other institutions responsible for capacity building in this field.
- Regional and international organisations that wish to support the cybersecurity capacity building of their member states with a view to strengthening national, regional, and global cybersecurity.
- Academia, civil society, ISPs, and the banking sector – as participants in consultations.

The big picture

One of the key principles of capacity building is to work from existing capacities and an understanding of where further capacity is needed. Clearly, this requires that existing capacities are assessed and understood before planning how to build on them. The practice presented here addresses this requirement.

Another important aspect of this practice is its comprehensive approach, which corresponds with the recommendation that capacity building is carried out in a systematic way, based on multiple criteria. The methodology used should be developed through a broad, multistakeholder collaboration, and should be a publicly available resource.

Equally important is the local ownership of the review process. The responsible governments must make the decision to carry out the assessment, and are responsible for using the results for making decisions and implementing recommendations.

Instructions

The country decides to carry out an assessment of its cybersecurity capacity. It should then look into existing models and explore which is feasible for the country's situation and whether cooperation with the institutions that conduct and facilitate those assessments is possible.

The steps vary depending on a model. In the case of the Cybersecurity Capacity Maturity Model for Nations (CMM) by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, the assessment is carried out by a team of the

institution providing a maturity model - or one of its partners once a country has requested and agreed on an assessment. The country then forms a host team, typically within a commission or a ministry, that is responsible for the organisation of the consultations. Possible challenges in implementation are related to limited funding and human resources, or to lack of political will and momentum.

An assessment can produce measurements for comparing the country's readiness with that of other countries, or produce a ranking; yet different models may have different outputs. The main purpose of assessments may be to provide a country with a 'health-check' and recommendations for future capacity building.

Timing

Timing depends on the model of assessment. For instance, in the case of the CMM, the assessment is a comprehensive review process composed of three-day in-country stakeholder consultations, and a review report based on the collected evidences and including recommendations. The whole process takes approximately three months.

Upon an agreement concluded with a country to carry out the review, the process takes about **three to six-week** preparatory phase which includes the organisation of venue and equipment, the selection and invitation of participants and preparatory desk research etc.

The preparatory phase is followed by a **three-day** intensive in-country review consisting of 9-10 sessions with in total 10 stakeholder clusters (including among others public and private sector, critical infrastructure, law enforcement, academia, and civil society).

The final **six-week** phase consists of the analysis of the focus group interviews and the drafting of a detailed report including recommendations, which is performed by the research team. This report is reviewed by a board of experts before the draft is shared with the country representatives for comment, feedback, and distribution.

Examples

The GFCE initiative "Assessing and developing cybersecurity capacity" is based on the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the GCSCC at the University of Oxford. The CMM was developed in consultation with more than 200 international experts from governments, international organisations, academia, the private sector, and civil society. It assists countries in understanding their priorities for investment and development by assessing cybersecurity capacity maturity across five dimensions: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training, and skills; legal and regulatory frameworks; and standards, organisations, and technologies.

The CMM deployment has been supported by the governments of the UK and Norway, and in cooperation with strategic partners such as the World Bank, the ITU, the CTO, and the OAS. It has been deployed in more than 50 countries to date. The

GCSCC is actively working on broadening the network of implementing partners and is currently developing a collaboration framework with regional partner institutions.

Countries interested in using this approach to assess their cybersecurity capacity maturity, and to plan further capacity building, can contact the GCSCC or one of its partners to discuss and initiate the process. For countries with limited means, there are possibilities for financial support which can be explored through the GCSCC. Once the review is agreed, the GCSCC or an implementing partner will guide the country through the process.

Other notable examples of maturity assessment are the ITU GCI, and the global CRI developed by the Potomac Institute. The GCI is a multistakeholder initiative to measure the commitment of countries to cybersecurity, through analysing five categories: legal measures, technical measures, organisational measures, capacity building, and cooperation. The CRI, on the other hand, is a methodological framework for assessing cyber readiness across five essential elements: cyber national strategy, incident response, e-crime and legal capacity, information sharing, and cyber research and development.

Source, support, and mentoring

The need for the use of methods such as the CMM, and their potential effectiveness is tackled in:

- Cyber Security Capacity: Does It Matter? A paper by William H Dutton and Ruth Shillair, Michigan State University – Quello Center, as well as Sadie Creese, Maria Bada and Taylor Roberts from the GCSCC: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-security-capacity-does-it-matter
- Cybersecurity Capacity Maturity Model for Nations: https://www.thegfce.com/initiatives/a/assessing-and-developing-cybersecurity-capability/documents/publications/2017/02/13/cybersecurity-cmm-for-nations

Several well documented examples of the CMM from countries are available online:

- Lithuania Cybersecurity Capacity Review 2017: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/lithuania-cybersecurity-capacity-review-2017
- Senegal: Cybersecurity Capacity Review 2016: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/senegal-cybersecurity-capacity-review-2016
- Madagascar: Cybersecurity Capacity Review 2016: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/cmm_rapport_final_cybersecurite_madagascar.pdf
- The UK Cybersecurity Capacity Review 2015: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/uk-cybersecurity-capacity-review-2015
- An example of follow-up steps taken on the basis of a review: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/kosovo-%E2%80%93-what-followed-cmm-review

More information on the ITU GCI:

- GCI 2017 Report: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx
- Country profiles: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx
-

More information on the global CRI by the Potomac Institute:

- Cyber Readiness Index 2.0 model: https://www.belfercenter.org/sites/default/files/files/publication/cyber-readiness-index-2.0-web-2016.pdf
- Country profiles: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

More information on the GFCE work:

- Assessing and Developing Cybersecurity Capability initiative: https://www.thegfce.com/initiatives/a/assessing-and-developing-cybersecurity-capability

Contact points:

- Carolin Weisser (carolin.weisser@oxfordmartin.ox.ac.uk)
- Robert Collett (Robert.Collett@fco.gov.uk)

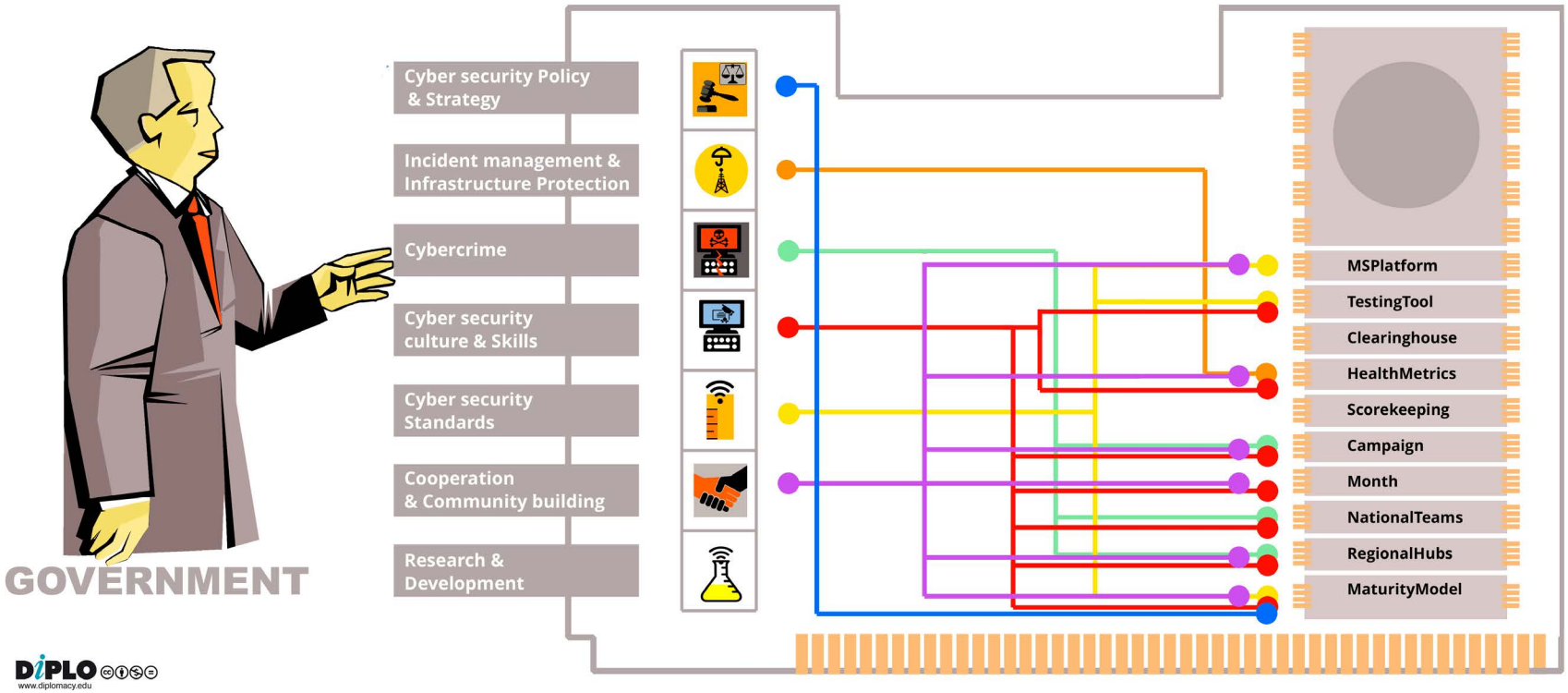
Annex I - Glossary

APCERT	Asia Pacific Computer Emergency Response Team
API	Application Programming Interface
APNIC	Asia-Pacific Network Information Centre
AS	Autonomous System
ASEAN	Association of Southeast Asian Nations
CB	Capacity building
CERT	Computer Emergency Response Team (see also: CSIRT)
CI	Critical infrastructure
CII	Critical information infrastructure
CIRT	Cyber Incident Response Team
CMM	Cybersecurity Capacity Maturity Model for Nations
CRI	Cyber Readiness Index
CSA	Cyber Security Agency
CSIRT	Computer Security Incident Response Team (See also: CERT)
CTO	Commonwealth Telecommunications Organisation
DDoS	Distributed Denial of Service
DNS	Domain Name System
ECDPM	European Centre for Development Policy Management
ECOWAS	Economic Community of West African States
ECSM	European Cybersecurity Month
FCO	Foreign and Commonwealth Office
GCI	Global Cybersecurity Index
GCSCC	Global Cyber Security Capacity Centre
GFCE	Global Forum on Cyber Expertise
GGPs	Global good practices
GLACY+	Global Action on Cybercrime Extended
ICT	Information and Communication Technology
ISAC	Information Sharing and Analysis Center
ISP	Internet service provider
ITU	International Telecommunication Union
ITU-ARCC	ITU - Arab Regional Cybersecurity Center
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
LACNIC	Latin America and Caribbean Network Information Centre

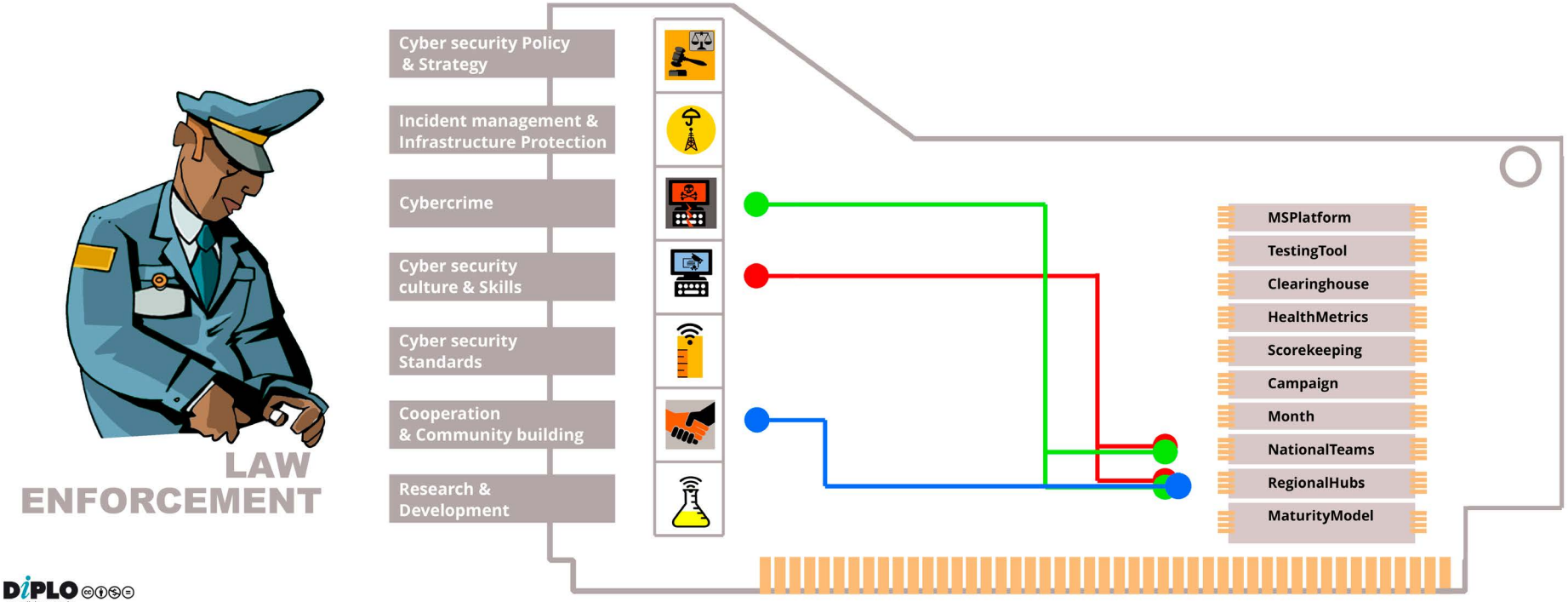
LEA	Law Enforcement Authority
NCSAM	National Cybersecurity Awareness Month
NCSC.NL	Nationaal Cyber Security Centrum of the Netherlands
NGO	Non-governmental organisation
NRA	National Regulatory Authority
NTP	Network Time Protocol
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OSINT	Open Source Intelligence
RIPE	Réseaux IP Européens Network Coordination Centre
RIR	Regional Internet Registry
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discovery Protocol
TF-CSIRT	Task Force on Computer Security Incident Response Teams
UNDP	United Nations Development Programme

Annex II - Visual navigation maps

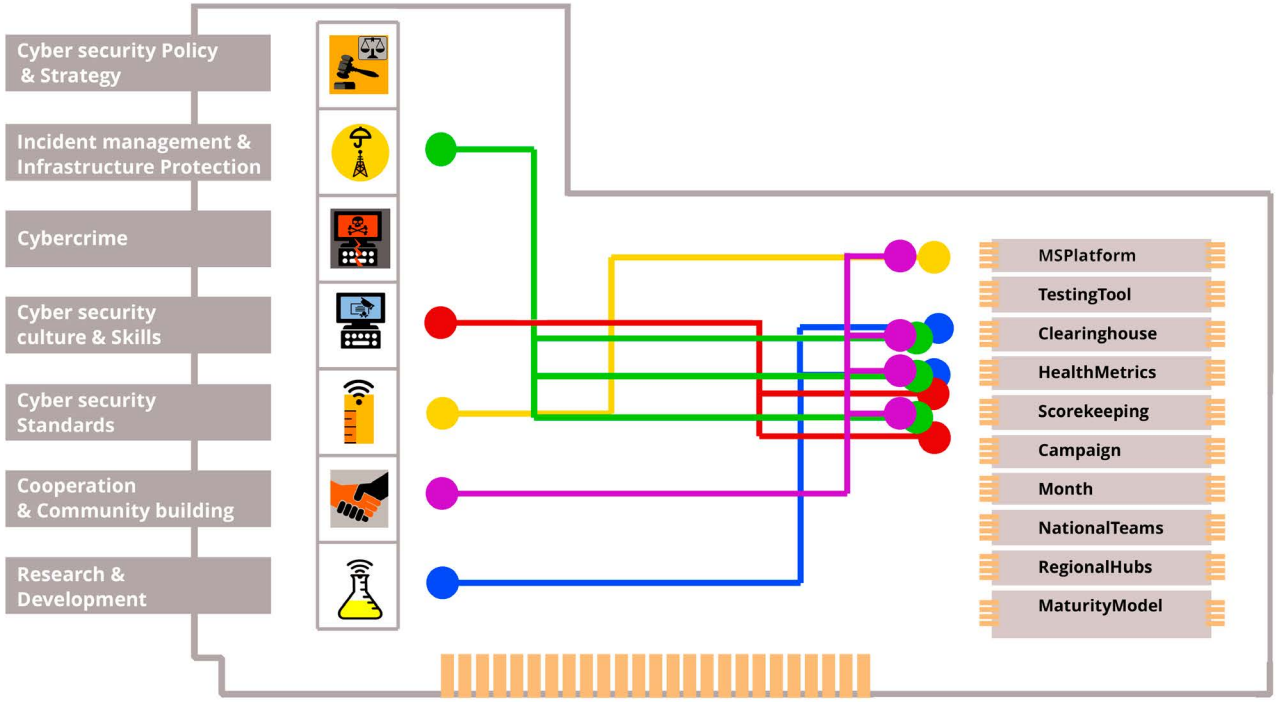
GGPs of particular interest to the governments



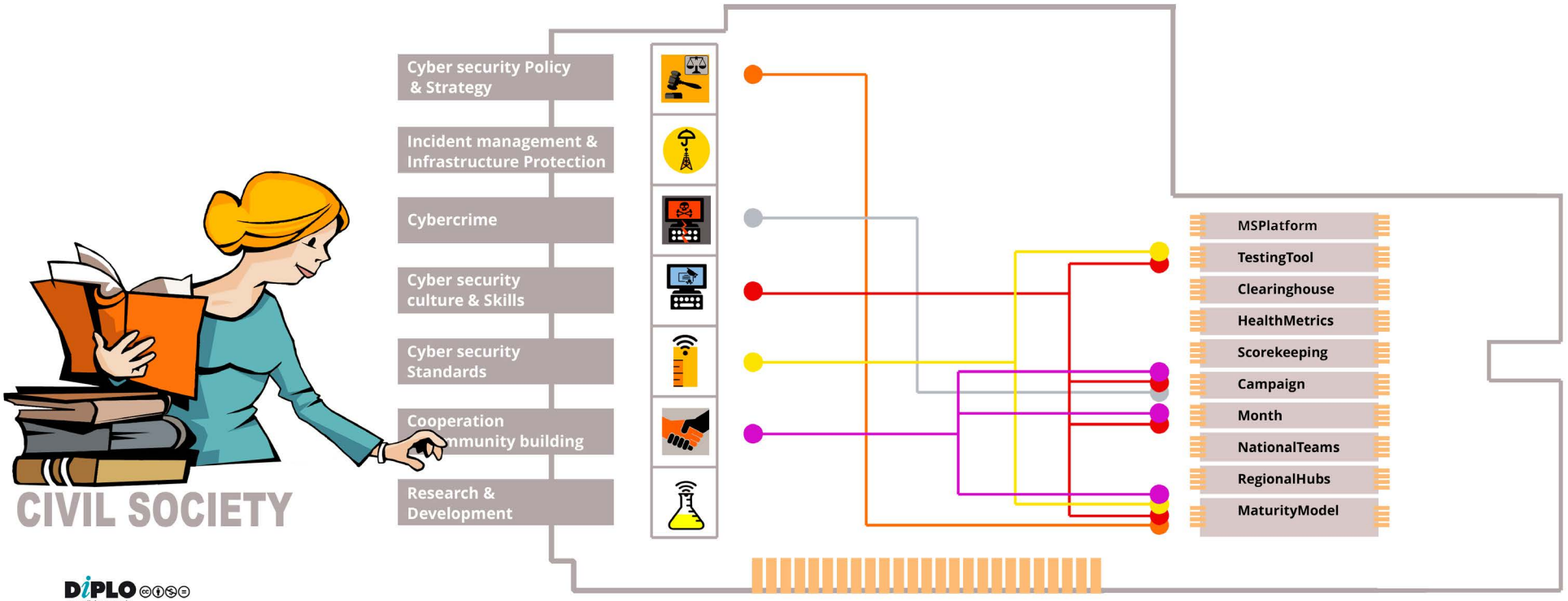
GGPs of particular interest to law enforcement authorities



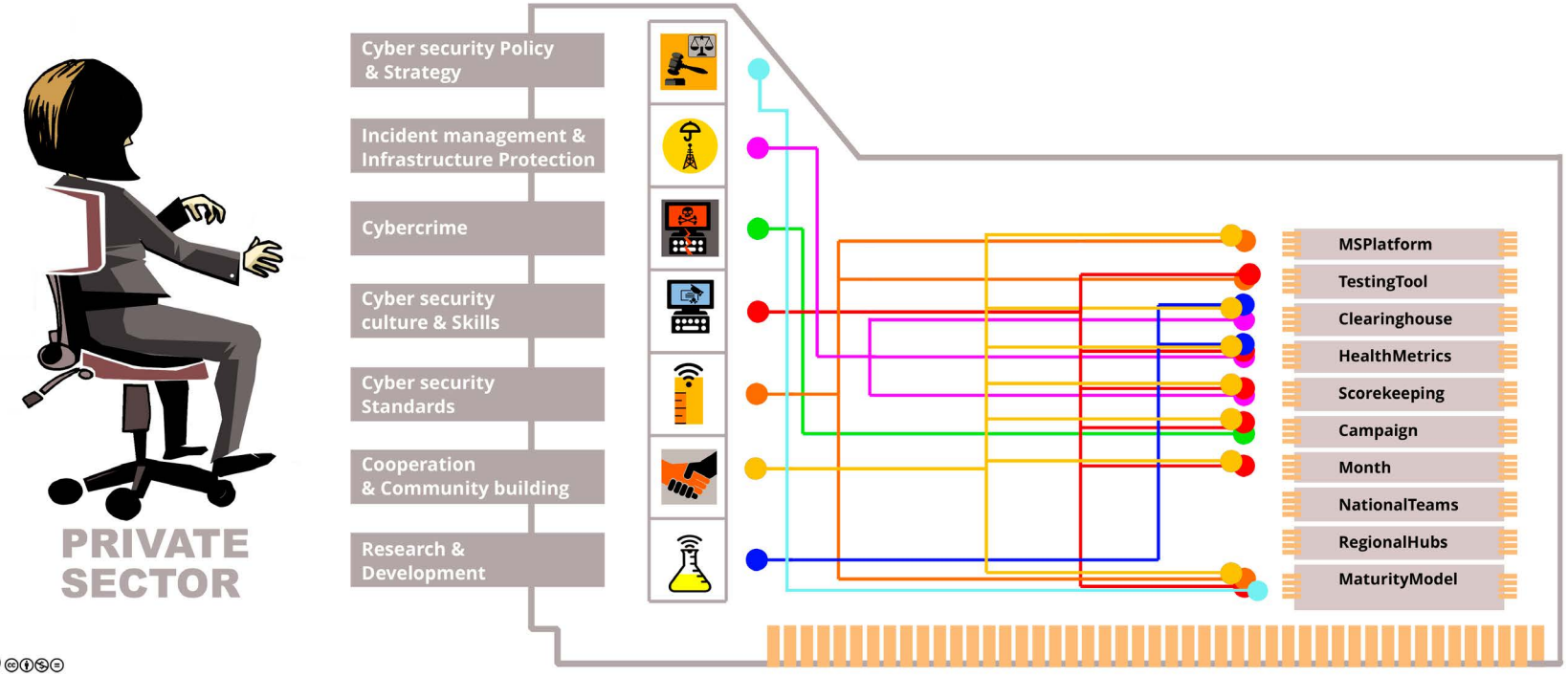
GGPs of particular interest to CERTs



GGPs of particular interest to civil society



GGPs of particular interest to the private sector



GGPs of particular interest to expert communities