GLOBAL PARTNERS DIGITAL
gp-digital.org

Unpacking the GGE's framework on responsible state behaviour: Capacity building

At the UN First Committee, two processes—the UN Group of Governmental Experts (GGE) and the Open-ended Working Group—are currently exploring the same question: responsible state behaviour in cyberspace. This term comes from a 2015 report by the previous GGE, which defines it according to a framework of four components: 1) norms, rules and principles; 2) confidence-building measures; 3) capacity-building; 4) the application of international law in cyberspace.

Understanding these components is crucial to engaging effectively at the GGE and OEWG. In this series, we'll be looking at each component in turn—looking at what they mean, how they have been defined, and their relevance to human rights. In this entry in the series, we examine the third component: capacity building. This explainer was authored by Klée Aiken of Asia-Pacific Network Information Centre (APNIC) and Sheetal Kumar of Global Partners Digital.

What is capacity building?

Capacity building has a wide range of definitions, even outside its application in cyberspace. According to one definition, it refers to "stimulating change by developing or strengthening the capabilities and competencies of individuals, institutions, governments and societies 'at large'", with an emphasis on the need for processes "to be driven 'from within' with external actors providing support" (UNDG[1] and EUISS[2]). In the context of cyberspace, capacity building—or, as it is often called, cyber capacity building (CCB)—can cover a wide range of efforts: from cyber maturity assessments and technical network operator training, to the establishment of institutions such as national incident response teams, cyber strategy and policy development, cybersafety awareness raising, and the development of e-government applications.

The UN First Committee's GGE on "developments in the field of ICTs in the context of international security", while not offering an exact definition of capacity building, has, over the course of its reports, made capacity building a key pillar of its recommendations to promote a secure and stable cyberspace.

This first consensus report delivered through the GGE process was in 2010, where capacity building received a relatively cursory but significant mention. Noting that "varying degrees of ICT capacity and security among different States increase the vulnerability of the global network", the group highlighted the "vital importance of capacity building to achieve success in ensuring global ICT security."

In 2013, the report outlined potential areas of focus for capacity building. These included topics such as the development of technical skills, legislation, strategies, regulatory frameworks, incident response capabilities, and awareness raising "to assist developing countries in keeping abreast of international policy developments".

As the group continued to refine potential areas of focus for CCB in 2015, the conceptualisation of capacity building also evolved. By the time the GGE's report came out, CCB was no longer being framed simply as an approach to secure the cyber ecosystem, it was now a direct means to operationalise the eleven non-binding norms included in the report and other recommendations of the GGE — with the group agreeing that "capacity building is essential for cooperation and confidence building" and suggesting that norm implementation "may not immediately be possible… until they acquire adequate capacity." Significantly, the 2015 report also allocated a space for the private sector, academia, civil society, and citizens within the discussion and delivery of capacity building.

The elaboration of capacity building through the GGE process has seen it mature to recognise the interconnected nature of cyberspace, and the roles stakeholders can play within it. The scope of capacity building expanded dramatically as well, from critical infrastructure security to policy and awareness raising.

So—to summarise—capacity building in the GGE context has come to refer to:

- A means to secure the cyber ecosystem directly (e.g through technical measures and policies);
- A means to action or realise cyber norms and confidence building measures; and
- A means to enable participation in cybersecurity discussions.

What do capacity building initiatives look like?

As previously outlined, there are a wide range of initiatives that encompass CCB. Although the GGE reports don't present an exhaustive list of potential activities, the recommendations within them highlight many of the most important areas of work around CCB, especially from the point of view of governments. These broadly fall under five themes:

1. Cybersecurity Policy

National Legislation/Strategy/Regulation: The development of national cyber legislation, straegies, and regulation can include awareness raising activities for policymakers, sharing of good practice and lessons learned, efforts towards harmonisation, initiatives to improve the policymaking process, and many more. For example, the Organization for American States' (OAS)[3] cybersecurity work includes research and outreach to policymakers as well as direct policy development support.

International Policy Engagement: The building of capacity within governments to understand and engage in international policy discussions is designed to facilitate more participation in global cybersecurity policy discussions, such as the First Committee processes, the GGE and OEWG. These include workshops hosted by the UN think-tank UNIDIR[4] to discuss key issues under discussion, and training materials developed by the Secretariat[5] for the processes. Beyond the spaces where norms are developed, initiatives such as the IETF policymakers program[6] look to bridge the gap between policymakers and the technical community, to foster better informed work on both sides.

2. Cyber Incident Management and Critical Infrastructure Protection

Critical National Infrastructure (CNI) Protection: Capacity building for CNI protection can include a range of measures: including CNI policy development; technical training; response drills; establishment and strengthening of information sharing platforms such as Information Sharing and Analysis Centers (ISACs); and other similar initiatives. The Meridian Process[7] is an example of a global governmental effort to share best practices around Critical Information Infrastructure Protection (CIIP).

Incident Response Teams: The establishment and strengthening of incident response teams (CSIRTs)—through technical training, site visits, facilitation of information sharing networks, dissemination of good practice, and other areas—has taken a central role in many CCB efforts, with a particular focus on national CSIRTs. Such initiatives include: good practice development, training, and fellowships by the Forum for Incident Response and Security Teams (FIRST)[8]; response exercises such as the annual APCERT Cyber Drill[9]; the establishment or strengthening of national incident response networks such as PaCSON[10]; and national initiatives to establish CSIRTs, as seen in Tonga[11], Papua New Guinea[12], and Vanuatu[13].

3. Cybercrime

Law enforcement capacity: Capability to combat cybercrime and cross border cooperation among law enforcement agencies are both important components of CCB. This often involves the development and adaptation of legislation, training for police, judges, and prosecutors, and other such efforts. The Council of Europe's Global Action on Cybercrime (GLACY)[14] is a capacity building program which incorporates all of these initiatives, building on the Budapest Convention on Cybercrime.

4. Cybersecurity Culture and Skills

Awareness raising: Awareness raising of cybersafety, cyber hygiene and cybersecurity issues can help users to use the internet safely and securely. These programs often target specific groups, including: new and at risk internet users; youth; seniors; private sector and government employees; civil society groups; and others. Such activities are often a high priority for local, national, and regional initiatives and may also include international partnerships, as seen under the STOP.THINK.CONNECT[15] program or regional efforts for local and training such as Cyber Safety Pasifika[16].

5. Cybersecurity Standards

E-learning and technical training: Technical training and e-learning programs are an important component of developing, maintaining, and securing digital infrastructure Technical training can take the form of hands-on training and technical assistance as delivered by organizations such as APNIC[17] or NSRC[18], technical best practice programs such as MANRS[19], and numerous other initiatives to help improve the skills across the workforce.

*

Finally, the sharing of good practice is a common theme across all areas of capacity building, with efforts such as the Internet Governance Forum (IGF) Best Practices Forums (BPF)[20] and the Global Forum on Cyber Expertise (GFCE)[21] helping to collect, develop, and disseminate good practices and expertise on various CCB topics.

What are the links between human rights and cyber capacity building?

Cyber capacity building processes are never neutral. They reflect the priorities, values, and approaches of those who design, deliver, and engage in them. From the prioritisation of work areas, to the metrics which measure and judge how secure systems and institutions are, and even the approach and framing of challenges, all aspects of CCB represent value judgements. For this reason it is important that any CCB initiatives are informed by a full understanding of their impact on society and human rights.

For example, CCB designed in a way that prioritises national security concerns risks propagating institutions, policies, and thinking that reflect and reinforce a narrow set of priorities. This can, in some cases, lead to measures which infringe human rights. Given the impact these developments have on the rights and lives of individuals and communities, it is important that CCB efforts adopt a holistic perspective.

By engaging in the design and delivery of cyber capacity building, human rights defenders can help institutionalise a multistakeholder and multidisciplinary approach to tackling cybersecurity challenges, which considers the impact on human rights.

As the links between human rights and CCB vary depending on the specific activity, they can best be demonstrated through examples:

1. Cybersecurity Policy

National Cybersecurity Strategies: National cybersecurity strategies provide an umbrella framework for a country's approach to cybersecurity. They can serve as an opportunity to get commitments from governments to human rights, and to ensure that a country's legal framework has comprehensive laws and regulations regarding data protection and privacy. They also offer an opportunity to ensure cybersecurity goes beyond national security concerns, to encompass issues of connectivity, access, awareness, as well as economic and social empowerment. This is also an area where human rights defenders have an important role to play. For example, those working directly with marginalised groups can bring their experience into the conversation.

2. Cyber Incident Management and Critical Infrastructure Protection

National Cybersecurity Centers (NCSC): An emerging trend to address cybersecurity across government has been the establishment of National Cybersecurity Centers (NCSC).

The work of incident response, requiring as it does quick information sharing, is dependent on strong relationships between different CSIRTs. For this reason transparency around linkages between CSIRTs and other parts of government—and a certain degree of independence—is important not only in helping ensure their operational effectiveness but, from a rights perspective, also to ensure that a CSIRT carries out its work in a way which doesn't undermine freedom of expression or privacy (this is dealt with in more detail in a paper by New America[22]). Human rights defenders can help by working for NCSCs to be established with strong transparency mechanisms, tailored to local needs, and with protections for the CSIRT's role and independence—by, for example, removing any mandate to filter traffic and content, gather intelligence, or conduct offensive activities.

3. Cybercrime

Law Enforcement Capacity Building: The development of cybercrime legislation and the training of law enforcement agencies, the judiciary, and prosecutors have perhaps the most visible intersection with human rights concerns. The definition of what is and isn't permissible online, and what constitutes criminal activity—particularly with regard to content—has strong implications for freedom of expression, privacy, assembly, association, and other rights. Training subsequently has direct impacts on the enforcement and legal interpretations of the legislation as well and rights such as the right to effective remedy. Equally, a lack of legislation, enforcement capacity, and cross-border cooperation can leave individuals at increased risk.

4. Cybersecurity Culture and Skills

Cybersecurity awareness campaigns: Ensuring that the public, companies and government employees have systems and processes in place to promote digital security, can consist of anything from government-sponsored workshops for employees, to public awareness campaigns, to trainings for company staff on issues such as strong passwords, safe storage of data and using encrypted email.

These efforts are key to ensuring a human-rights respecting cyberspace, because—without digital security awareness—users will be putting themselves and others at risk. Further, awareness campaigns themselves should be human rights-respecting, and should not be used to restrict the use of the internet to access information—for example by discouraging the use of the internet for accessing information about sexual health or other sensitive topics.

However, because behaviour change is complex, it is important that these campaigns are both sustainable and responsive to the particular context in which they're being delivered. In other words, they should be targeted and practical. Many human rights defenders provide digital security training for at-risk groups, including indigineous communities, other human rights defenders, journalists and members of sexual, ethnic or religious minority groups at risk of surveillance or harassment by authorities. With their experience in providing these trainings, human rights defenders can be seen as important resources in the delivery of cybersecurity awareness campaigns, particularly for at-risk groups.

5. Cybersecurity Standards

Technical standards: Although a contentious space, the divide between technical implementation and human rights is increasingly being recognised, and has implications for standards related to capacity building. The IRTF Human Rights Protocol Research Group[23], for example, is exploring the ways internet protocols can have both enabling and degrading impacts on human rights. Capacity building on the development and implementation of technical protocols, and standards around issues including encryption, machine learning algorithms, and other areas, have implications for the rights to privacy, freedom from discrimination, association, and of expression, among others.

*

The delivery or implementation of CCB is where the most tangible contributions can be made. However, where securitisation of the narrative is increasingly prevalent, it is also valuable for human rights defenders to engage in the formulation of the narrative, and not simply in reaction to the results on the ground.

This is where the UN First Committee processes—the OEWG and GGE—are particularly relevant. Although direct on-the-ground impact can be difficult to quantify, discussions and outcomes of these processes reflect international consensus, and can therefore shape the set-up and implementation of CCB at the national level. For example, similar to the inclusion of respect for human rights in the norms which are included in the 2015 report, a similar linkage could be advocated for explicitly in regard to capacity building. Further, the recognition of the importance of a holistic and multistakeholder approach to capacity building in such high-level spaces can have an impact on the priorities and approach of funders and implementers of CCB, and thereby on the project design and on the delivery of CCB.

End notes

1. UNDG, https://undg.org/document/capacity-development-undaf-companion-guidance/
2. EUISS, https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building
3. OAS, http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp
4. UNIDIR, http://www.unidir.org/est-cyber
5. UN Secretariat, https://www.un.org/disarmament/ict-security/
6. IETF Policymakers' Program, https://www.internetsociety.org/fellowship/ietf-policy-program/
7. Meridian Process, https://www.meridianprocess.org/
8. FIRST, https://www.first.org/
9. APCERT, https://www.apcert.org/
10. PaCSON, https://www.cyber.gov.au/
11. Tonga CERT, https://blog.apnic.net/2016/07/20/lessons-establishing-national-cert/
12. Papua New Guinea CERT, https://blog.apnic.net/2017/11/21/strong-start-png-cert/
13. Vanuatu CERT, https://blog.apnic.net/2018/07/09/busy-six-months-ends-in-cert-vanuatu-launch/
14. GLACY, https://www.coe.int/en/web/cybercrime/glacyplus
15. STOP. THINK.CONNECT, https://www.thegfce.com/initiatives/g/global-campaign-to-raise-cybersecurity-awareness
16. Cybersafetypasifika, https://www.cybersafetypasifika.org
17. APNIC, https://www.apnic.net/
18. NSRC, https://nsrc.org/
19. MANRS, https://www.manrs.org/
20. IGF Best Practices Forum, https://www.intgovforum.org/multilingual/content/best-practice-forums-4
21. Global Forum on Cyber Expertise, https://www.thegfce.com/
22. New America, https://www.newamerica.org/cybersecurity-initiative/policy-papers/national-csirts-and-their-role-in-computer-security-incident-response/
23. IRTF Human Rights Protocol Research Group, https://irtf.org/hrpc