DiploFoundation

Comments on the initial 'Pre-draft' of the report of the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security

Contribution by DiploFoundation

Comprehensive Capacity Building

April 2020

Capacity building is seen as the third pillar of international cybersecurity policy, along with norms and rules, and confidence building activities, which was clearly recognised by the UN Group of Governmental Experts (GGE) as well as regional organisations; the Organization for Security and Co-operation in Europe (OSCE), the ASEAN Regional Forum (ARF), and the Organization of American States (OAS). They also all recognise that the implementation of norms and capacity building measures (CBMs) are not possible without strong capacity of states and other stakeholders. Nevertheless, capacity building is often the last item on the agenda, around which a very general agreement can easily be made, but lacking deeper understanding of what is needed - as well as concrete follow-up to commitments.

With 20 years of global experience in conceptualising and delivering capacity building programmes in diplomacy and digital policies, including in the cybersecurity field; DiploFoundation is encouraged to support the Open-Ended Working Group's (OEWG) deliberations by sharing its 'lessons learned' and propose several principles to be taken into consideration in the final report, as well as possible practical steps that may follow.

The following contribution provides inputs to Section F 'Capacity-building' of the OEWG Initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. The contribution provides suggestions for the principles that should guide the ICT-related capacity building efforts, as proposed in Section H 'Conclusions and Recommendations', Article 68 d in particular.

Geneva 7bis, avenue de la Paix, 1202 Geneva 2, Switzerland | *t.* +41 22 741 0420, *f.* +41 22 731 1663
Malta Ground Floor, Anutruf, Hriereb Str, Msida, MSD 1675, Malta | *t.* +356 21 333 323, *f.* +356 21 315 574

DiploFoundation

The principles that should underpin ICT-related capacity building efforts in the field of international security:

1) "Triple-Multi" approach to capacity building

Multidisciplinary and holistic approach

A multidisciplinary palette of knowledge is needed – related to technology, legislation, and diplomacy – to address preparedness, respond to incidents, avoid miscommunications, and implement international law. In addition, the norms and CBMs themselves require a holistic understanding of the cyber environment by involved stakeholders; including topics outside the narrow scope of security – in particular, human rights, freedoms, and economic growth.[1] Embedding perspectives of developing countries within capacity building programmes is of particular relevance. This does not only mean targeting developing countries' stakeholders as beneficiaries, but also introducing developing world perspectives into the curriculum and methodology, targeting everyone (e.g. understanding different political, economic and cultural context, risks related to regional conflicts and tensions, and specificities of developing digital solutions across various developing regions - anchored to the Development Agenda 2030).[2]

Multistakeholder approach

Partnership between diverse stakeholders on capacity building is needed:

- as beneficiaries (e.g. diplomats on cybersecurity, and tech industry on diplomacy)
- as sponsors (e.g. states and private sector to act jointly as donors, particularly for developing countries)
- as implementers (e.g. capacity building organisations and academia to assist international organisations and private sector on conceptualising and delivering capacity building)
- as knowledge repositories (e.g. cutting-edge knowledge of private sector, technical community, research institutions and think-thanks, in particular through existing international fora like the Global Forum on Cyber Expertise (GFCE)
- for outreach (e.g. civil society outreach to wider communities and national and regional stakeholders that should play their role)

Broad co-operation of governments and the private sector towards increasing the resilience and security of digital products and services will be of particular relevance - especially as the framing of critical infrastructure gets blurred by crises which show that some unexpected and emerging digital sectors (like e-commerce, or online conferencing platforms) can suddenly become supercritical in specific circumstances.[3]

[1] Cybersecurity Competence Building Trends, DiploFoundation (2016): https://www.diplomacy.edu/sites/default/files/Cybersecurity%20Full%20Report.pdf
[2] Towards a secure cyberspace via regional co-operation, DiploFoundation (2017): https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf
[3] Geneva Dialogue on Responsible Behaviour in Cyberspace: https://genevadialogue.ch/

Multilevel approach

To be effective and comprehensive, capacities need to be developed on various levels. The key international developments related to shaping new instruments certainly take place on the global level - primarily at the UN GGE and OEWG, but also in the other international organisations like: the International Telecommunication Union (ITU), the World Trade Organization (WTO) or the United Nations Educational, Scientific and Cultural Organization (UNESCO); and multistakeholder fora like the Internet Governance Forum (IGF), the GFCE, Internet Engineering Task Force (IETF), and the Internet Corporation for Assigned Names and Numbers (ICANN). Stakeholders ought to develop capacities to participate meaningfully in these processes and 'connect the dots'. Main security challenges of digital transformation are also felt on national and local levels; where governments need to work with stakeholders to establish local policies and mechanisms that require the development of normative, operational, and co-operational institutional capacities adjusted to local needs. Regional co-operation, however, is often side-lined, in spite of the fact that it is regional tensions - not global ones - that often turn into violence and conflicts; and cyber will increasingly become a tool for this. Capacities for establishing regional co-operation and developing trust based on digital co-operation are of particular relevance for peace and stability.[4]

2) *Capacity building as a process*

Comprehensive approach

Development of hard and soft capacities requires carefully designed training, coaching, and organisation building activities. In this regard, capacity building goes beyond simple training, and requires to be set up as a long-term and sustainable process consisting of training and courses; policy immersion; coaching and help desks; research and monitoring; observatories; and nurturing established communities. As debates on cyber policies have shifted to a more mature phase, a stronger focus on organisational development is required. This includes developing organisational capacities of governments, civil society, business associations, and academia among others.

Sustainability

To reflect the demand to implement capacity building as processes rather than events, there is a need for sustainability of capacity building endeavours. This can be achieved through budgetary planning, commitment, and investments by states and regional organisations; the involvement of the private sector, civil society, and academia in conceptualising and implementing the programmes[5]; and by including cybersecurity aspects as well as digital literacy in the curriculum of academic and professional training centres.

In addition, better co-ordination on capacity building efforts by donors and international and regional organisations, where the UN bodies and fora - including the IGF, regional organisations, and global multistakeholder alliances like the GFCE, is needed.[6]

---

[4] Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities, Diplo Foundation (2016): https://www.diplomacy.edu/sites/default/files/Cybersecurity%20in%20Western%20Balkans.pdf

[5] GFCE Global Agenda for Cyber Capacity Building, Global Forum on Cyber Expertise (2017): https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf

[6] Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities, Diplo Foundation (2016)

3) Innovations and creativity

'Going online': Online formats and methodologies

The ongoing Coronavirus pandemic has underlined what has been discussed, but rarely implemented for years: that capacity building needs to embrace online tools and methodologies, and not be limited to 'photo opportunity' events. Online courses, discussions, webinars, roundtables, help desks, observatories, and other modalities should become an integral part of a blended-learning approach. This shift, however, requires more than embracing technology and tools which is readily available: it requires substantial investment in sharing existing good practices of online capacity building frameworks, and research on how to adapt real-world 'normals' to the emerging 'new normal' which includes increased social distancing.

Creativity in capacity building

Evolving 'fast speed' working practices - driven primarily by the spread of digital technologies but also the evolving crisis - further shrinks the (already limited) attention span for learning, and amplifies the 'paradox of plenty' of the information age (being increasingly incapable of utilising the value of abundance of information, including literature, research work, crash courses, etc). Therefore, creativity in delivering capacity building is becoming critical. Strong investment by governments and the private sector is needed in exploring creative ways to deliver capacity building, in particular through partnerships with leading capacity building institutions.

The OEWG and regional forums should continue to outline key capacity building requirements and needs, and propose particular co-operation measures. More importantly, they should also move out from normative grounds to the practical implementation of comprehensive capacity building programmes, in partnership with academic institutions, civil society, capacity building and training organisations, the private sector, and the technical community.

DiploFoundation remains devoted to supporting continuous international efforts in the field of ICTs and international peace and security - through its landmark projects: Geneva Dialogue on Responsible Behaviour in Cyberspace,[7] the Geneva Internet Platform (GIP) just-in-time courses and assistance for diplomats,[8] the *GIP Digital Watch* observatory and its dedicated page following developments of the GGE and OEWG,[9] and online courses and webinars related to cybersecurity policy and international co-operation;[10] all with support of the Government of Switzerland and other partners.

DiploFoundation also remains available for additional inputs and endeavours, invites for new partnerships in the field, as deemed necessary.

[7] Geneva Dialogue on Responsible Behaviour in Cyberspace: https://genevadialogue.ch/

[8] The Geneva Internet Platform (GIP): https://www.giplatform.org/

[9] UN GGE and OEWG, GIP Digital Watch observatory: https://dig.watch/processes/un-gge

[10] https://www.diplomacy.edu/cybersecurity#training and https://www.diplomacy.edu/cybersecurity#events