Capacity building in cyberspace: taking stock

A seminar organised in the framework of the EUISS Cyber Task Force
Brussels, 19 November 20013

Event Report

Background

The purpose of this meeting was to bring together various communities with a stake in cyber capacity building. The focus on cyber capacity building served as a bridge for engaging across various policy areas, including foreign policy, development, the digital economy and cybercrime.

Main points

The participation of government officials, analysts, business and civil society representatives facilitated a better understanding of the policymaking challenges in this area, including the conceptualisation and taxonomy of cyber capacity building, identification of models for structuring cooperation between the public and private sectors, and gaining a clearer view of the needs of recipients. The following main points emerged in the discussions:

- *Capacity building in cyberspace should follow a multi-level governance process*, encompassing not only 'vertical' training but also a horizontal effort across government departments, the involvement of private actors, and civil society. The EU's engagement on capacity building is a very welcome development but needs to take into account the context within which the recipients operate.
- *There is a general wish for better identification and assessment of the ongoing capacity building projects* in order to allow for a more efficient and coordinated allocation of resources. In order to have a meaningful discussion, it is necessary to develop a taxonomy and vocabulary (common or individual).
- *Mainstreaming cyber capacity building into development programmes is essential but also challenging***.** The benefits of an open and secure internet for economic and social development need to be presented in a clear way in order to make sure that mainstreaming cyber-related issues does not become an 'empty shell'. Developing methodology for assessing cyber capacity building efforts remains a big challenge.

Follow-up activities

The EUISS, in cooperation with the European External Action Service, will organise *a capacity building conference on 13-14 March 2014 in Paris. This event will focus on the role of regional organisations in cyber capacity building. The aim of the conference is to discuss the link between various dimensions of cyber capacities and development policies.*

Participation in this event will be open to government officials, representatives of international organisations, civil society and the private sector from developed and developing countries (about 50-60 people). The event will be split into working sessions (13 March) and high-level panels (14 March).

More details will be circulated to member states and EU institutions in January 2014.

Summary of individual sessions

- *Panel 1: Defining capacity building in cyberspace*

The first panel discussed *the need for a global engagement on cyber capacity building*. The general agreement emerged that capacity building is something that should leave recipient countries with the ability to enjoy the benefits of cyberspace, including in the economic and social domains. Such an endeavour should be flexible and adopt an interdisciplinary approach.

One speaker highlighted the *need for the EU to engage globally* in order to preserve open and secure cyberspace. The panel agreed that *diplomacy* performs a very useful function in inspiring nations to build capacity and encourage political will to follow through on commitments. In its *development programmes*, the EU must consider investing in cyber capacity building as one of its priorities. However, one speaker warned of the difficulties surrounding the idea of *mainstreaming* cyber security into development programmes, as it is rarely done well. It often dilutes goals and ends up being discussed in a range of international fora yet little is achieved. Therefore, the involvement of the development community is essential.

It is important to develop *common concepts* of cyber capacity building. A working definition proposed by one of the speakers saw capacity building as '*support provided to developing nations to increase their access to, and ability to fully benefit from, the internet and other elements of cyberspace*'. Therefore, projects that use ICTs to achieve other ends are not necessarily cyber capacity building projects. It was also proposed to develop a portal for information sharing, which could be a practical outcome of the task force, provided the issue of the ownership of such a portal is properly resolved.

Also it is important to figure out a way to *gather and map data on cyber capacity building projects.* This would help to implement s*tandards* and a common set of concepts. The European Network and Information Security Agency (ENISA) does some work in this regard. It facilitates the exchange of information between, and develops technical guidelines for, EU institutions, the public sector and the private sector.

Cybersecurity must be a collective endeavour and proceed in an *interdisciplinary way*. A speaker outlined the need for interaction between cyber experts and non-experts alike, for a scientific approach, and for an open debate. Capacity building goes beyond some of the common narrow assumptions about cybersecurity, in particular the focus on cybercrime, training of national police or replicating legal standards. The speaker argued that cybersecurity should begin with a strategy that is appropriate for the individual country. Capacity building is about more than a focus on Europe – it must focus first and foremost on *the needs of the people*.

The ensuing discussion highlighted some of the *challenges of the comprehensive approach to capacity building.* One speaker discussed the risk of promoting an EU-centric model and another pointed out that not every country within the EU has an advanced level of cyber capacities.

During the discussion a question was asked as to what extent approaches adopted towards recipient countries should be linked to a clearly defined purpose (i.e. an open and secure internet). A discussant suggested that – given the importance of the subject - the EU should perhaps think of setting certain red lines for providing assistance. The speaker responded that the EU should not be too rigid in the approach it adopts. The reality is that as a donor, the EU does not operate in a vacuum and so must be prudent; recipients can go to China for funding if they feel the EU is expecting too much from them.

The panel agreed that we will have achieved *good, sustainable and scalable capacity building* when the need is understood at all levels – among the citizenry, government, and institutions. A comparative assessment or a risk analysis could also be used to measure success.

- *Panel II: Capacity building and security of ICTs*

The second panel discussed how cybersecurity is a *shared responsibility within the EU*. They spoke about building cyber capacities through public-private partnerships and in doing so building confidence and security in the use of ICTs.

The panel started with the discussion of main trends in cyberspace. In the next seven years, another 2 billion users will come online globally. Similarly, the growth of cybercrime over the past few years has been unprecedented. Because of the global and interconnected nature of cyberspace, governments and the private sector alone cannot combat all these threats. Furthermore, both entities have a collective responsibility for safety and preparedness and so *a public-private partnership model* needs to be effective. Private sector input should be sought more in the policy planning stages because private industry owns much of the ICT infrastructure and is most active in the development of new technologies. Public-private partnerships should begin with a clear purpose, define roles and responsibilities, raise awareness of threats, foster continuous training, build trust in cooperation, share costs and resources, avoid 'mission creep', and wind the project up when all of the objectives have been achieved.

Globally, needs, legislation and regulations will vary. One speaker illustrated *a hierarchy of requirements for internet users* and how cyber resilience is important at each level. This hierarchy provides a framework to prioritise national cybersecurity efforts, looking at *access, resilience, connectivity* and *trust,* in order to build an optimum level of security on the internet for government, industry, and civil society. At each tier, a user is engaging with the internet in a different way, and cybersecurity has a role to play.

The panel fielded questions on translating cybersecurity into direct action. There was broad agreement that action taken would depend on the specific profile of each country. Policymakers should assess whether cybersecurity has traditionally been a priority, and more importantly whether the country concerned has the capacity to deal with it.

The panel also discussed the positive and negative effects of a private sector consultancy role in government. The panel felt that the private sector is not in the business of taking over the policy role from governments or dictating legislation. As the private sector built and owns most of the infrastructure, there is a need for governments to assert a more proactive role and engage in a more robust dialogue on what works. E-government policies increase the demand for private sector involvement.

- *Panel III – Cybersecurity, norms and values*

The final panel considered how to transpose the rule of law to cyberspace. The diverse activities taking place in cyberspace build on sometimes conflicting social and legal norms, which challenge a unique understanding of cybersecurity. The panel addressed *cybercrime and the law enforcement efforts* of Europol, Interpol, the Council of Europe, and the role of OIDHR. A number of recommendations were made on how to harmonise law enforcement methods between countries both EU-wide and beyond.

On the *freedom-security nexus,* one speaker argued that if freedom of expression and other fundamental rights apply in cyberspace then there is also space for crime to thrive. Cybercrime operates in a borderless space and so presents new challenges for law enforcement. The European Cybercrime Centre (EC3) seeks to uphold freedom on the internet. Their focus is on safeguarding privacy and the right to anonymity in cyberspace. If this freedom is abused, perpetrators should be punished and so a need exists to contact the

end user. To uphold the right to privacy, a robust framework and procedure for tracing data involving end users (and culprits) must exist, thus enforcing responsibility.

To get law enforcement capabilities at a comparable level throughout the EU, a speaker suggested a new penal law standard for cybersecurity with minimum e.g. web-filtering technology used to combat child sexual abuse as a blueprint, standardisation, continued support for EC3, cooperation with third parties, and more training in national law enforcement at EU level e.g. CEPOL.

Another speaker highlighted the *multi-stakeholder environment* already in play in the EU and beyond, especially in the training and capacity building framework i.e. EC3, CEPOL, and Eurojust. *The Council of Europe approach* to cybercrime involves a broad array of instruments: setting and making use of cyber standards globally (The Budapest Convention, a joint EU-CoE Global Action on Cybercrime - GLACY) and the performance of assessments (Cybercrime Convention Committee, Capacity Building Programmes).

The Interpol Global Complex for Innovation, to open in 2014, will be seeking to identify trends, build capacity in cybercrime units, and facilitate international cooperation in cyber-operations. It will build awareness and training for executive law enforcement officers and foster links with technology partners.

Cyber capacity building is also important for implementing *secure ways to interact with government*, e.g. new voting technologies. To transform an instrument created for paper-based procedures into an electronic form creates challenges: if no encryption is used, for instance, the vote becomes traceable. The OSCE–ODIHR works to create confidence for electoral candidates and voters alike, enhance the integrity of the process, and deter possible fraud and intimidation. It is process-oriented: results matter to the degree that they are reported honestly and accurately. The OSCE-ODIHR assesses compliance with international standards e.g. free, secret, and universal elections, and recommends ways in which electoral processes can be improved.

Although some governments lack full awareness of the threat landscape, issues such as fraud are already part of the public discourse. *It is important for capacity building* to change the perception of governments as inherently unable to effectively deliver on electronic capacities, e.g. e-voting.

One participant asked how the various organisations deal with *cybercrimes with a political dimension.* Interpol does not issue a 'red notice' in such cases. They refuse to deal with political issues as Interpol has 190 members – not all of them democracies. Within the EU, national security remains the prerogative of member states and therefore state-sponsored cyber attacks are dealt with by member states. An open-ended debate was generated by the issue raised by another participant, namely to what extent private companies should be held liable for security failures

Key sources mentioned during the event

- EU Cyber Security Strategy: open, safe and secure cyberspace
- Convention on Cybercrime (CETS No.: 185)
- Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union (NIS Directive)
- 2013 Seoul Cyber Conference
- EUISS Policy Brief on Cyber ('Cyber world: site under construction', September 2013)
- EY's Global Information Security Survey 2013
- Microsoft reports: 'Linking Cybersecurity Policy and Performance' and 'Hierarchy of Cybersecurity Needs'