Building security capacities in cyberspace: What lessons from other policy areas?

26 September 2014, Paris
10:00 – 17:00

Several policy areas have substantially benefited from the rollout of ICT in the past decade. So far, the main focus has been on ensuring the efficiency of those policies and on maximising their contribution to human development and economic growth. More recently, however, security experts have stressed the importance of secure and resilient ICT networks and systems – in both developed and developing countries – as a precondition for the overall success of investments in ICT projects[1]. Potential risks vary from mobile spoofing and data breaches to attacks on critical infrastructure, including energy or water networks. Dealing with this new reality first requires acknowledging that development objectives and risks related to ICT networks are two sides of the same coin, and need to be addressed in a more comprehensive and coordinated manner. From the perspective of the security community, this implies that cyber resilience must be a component of all cyber capacity building projects if development efforts are to be successful. That also means that different communities – the cybersecurity community, the ICT4D and others – have to be able to work together effectively.

Aim

The purpose of this meeting is to discuss the role of resilience and security within a broader vision for cyber capacity building: what do we ultimately want to achieve and how do we get there? For instance, would adopting a comprehensive and coordinated approach to capacity building that integrates the elements of resilience into other policy areas be a desirable option? Or are we instead destined to see the emergence of a prevailing model of fortified islands[2]?

In pursuing a specific model, what can we learn from experiences with capacity building in other policy areas, i.e. ICT development, security sector reform, counterterrorism? For instance, what can we learn from the human rights mainstreaming (i.e. systematically integrating HR in sectors like energy, transport or environment) that is broadly promoted by the OECD Development Assistant Committee (DAC).

Multiple examples suggest that such an exchange of experiences could be a fruitful and beneficial exercise. This could help to address the fact that, for instance, elements of cyber resilience are currently excluded from security sector reform initiatives (i.e. reforms of police, border management, customs, etc.). However, given the resources committed by the international community to building capacities in the fight against cybercrime, could we envisage creating linkages between those efforts, and if yes, on what conditions? At the same time, we stand to learn from the development community's engagement of more than a decade in promoting the use of ICT to achieve its goals. With a clear link to other policy areas such as agriculture or education, how are different actors brought on board and what are the lessons from those engagements?

[1] For the purpose of this note the terms cybersecurity and cyber resilience are used interchangeably.
[2] Another metaphor that is common in the US is the notion of 'baking security in' vice 'bolting it on' treating it as 'icing'.

Method

To facilitate and frame the discussion, we will circulate a background note with different scenarios for engagement between cybersecurity actors and other capacity building communities. These include:

- ***Desert islands***: policy communities (cyber, development, law enforcement) organised according to their mission and policy objectives. They are often suspicious of the motives of other communities or consider opening up their network to be a waste of time and resources. These communities operate based on the assumption that they are in control of the resources needed for the attainment of their objectives

- ***Fortified Islands:*** groups that incorporate security/resilience elements in their objectives on a case-by-case basis, depending on the policy area. They emerge mostly in response to a problem that cannot be addressed adequately within one group because the required resources – financial, knowledge or otherwise – are spread across different communities

- ***Security Archipelagos:*** formations in which interactions between the cybersecurity community and others take place on a regular basis but are still limited to a carefully selected set of issues. The continuity and regularity of cooperation is the primary difference to the fortified islands which perceive security as an 'add-on' to their activities rather than an integral element. Such initiatives are usually expected to continue in the future and from the outset aim at making cyber-related issues an integral part of any cooperation efforts

- ***Continental drift:*** represents the most advanced form of cooperation. They are characterised by both the diversity of actors – which helps to ensure adequate access to resources and knowledge – and the incorporation of other aspects of cyber policy as an integral element in achieving objectives identified in other policy areas. This could be also described as an integrated capacity development model, whereby a joint effort is made by all parts of the network.

The intention of this meeting is to bring together experts across several disciplines in order to extrapolate the lessons learnt from capacity building in other policy areas and discuss their implications for capacity building in the realm of cybersecurity.

Consequently, the discussion will be organised along three main themes:

- Decisions on membership of a given initiative
- Choice of a method for merging various policy objectives
- Selection of a suitable format for the initiative

In addition, we would like the participants to reflect upon a broader set of questions which may be useful for framing the discussion:

- What are the priorities of your policy community with regard to ICT?
- Are the cybersecurity and resilience elements part of their capacity building initiatives? If so, in what ways?

AGENDA

10:00 – 10:30 **Registration and coffee**

10:30 – 11:00 **WHERE ARE WE HEADING?**

The focus of this session will be to discuss the proposed scenarios and assess the current situation – and final destination – of the cyber capacity building community. The aim of this session is explore the advantages and disadvantages of different options from the perspective of various policy communities. The outcome of this short debate will help set the scene for the successive sessions, which will aim to shed some light on future options.

Presentation of scenarios
Patryk Pawlak, Senior Analyst, EU Institute for Security Studies

11:00 – 17:00 **ARE WE THERE YET?**

10:30 – 11:45 **Membership: who is in, who is out?**

One of the key challenges for the cyber capacity building community is the bringing together actors with different cultures and policy objectives in order to build constructive relationships between them. This does not imply an 'all in' approach by default, but involves a decision about who to include and who to leave out (and for what reasons) from a specific initiative. While homogeneous groups (i.e. bringing only technical experts or only development actors) tend to foster cooperation between their members, heterogeneous ones (i.e. bringing together development and cyber experts) often pose more of a challenge, especially where trust is lacking between members with regard to the objectives of a given community.

Questions: *What elements guide the decisions about membership, especially in case of cyber capacity building?*
If membership is not an option, what are the alternatives for cooperation and improving understanding among different communities?

Impulse givers **Laurent Bernat**, Cyber Security Risk Policy Analyst, Directorate for Science, Technology and Industry, Organisation for Economic Co-operation and Development (OECD), Paris
Samia Melhem, Lead ICT Specialist, World Bank, Washington, D.C.

11:45 – 13:00 **Method: isolation, cherry-picking or mainstreaming?**

With a growing application of ICT, in different spheres of human activity it is important to look into methods for effectively including cyber resilience across a range of policy areas, including agriculture, energy, transportation, education and health. Although specific risks for each of them vary, they all share the urgency to take the cybersecurity aspects into account. Even though there is no 'one size fits all' solution to cybersecurity problems, and no single cyber capacity building model, there are elements which – with some adaptation – can be universally applied. While individual components of existing frameworks are case specific, the overall approach and objectives can be replicated. Looking at the existing and potential methods for incorporating cyber resilience elements into other policy areas, it is possible to distinguish different degrees of that process, including isolationism, cherry-picking, and mainstreaming.

Questions: *What are examples of methods applied by different countries and organisations?*
What lessons can we draw from those experiences?

Impulse givers **Marcin de Kaminski**, Policy Specialist – Freedom of expression/ICT, Swedish International Development Cooperation Agency (SIDA), Stockholm
Guido Gluschke, Managing Director and Senior Research Fellow, Institute for Security and Safety, Brandenburg University of Applied Sciences, Potsdam

13:00 – 14:30 **Working lunch**

Update by the Netherlands on Cyber Conference 2015

Update by the European Commission and EUISS on the cyber-needs conference

Update by the Global Cyber Security Capacity Center on the Cybersecurity Capacity Portal

14:30 – 15:45 **Format: hierarchy or networks?**

Relationships between actors can usually be arranged as hierarchical structures or networks – both serving different purposes. Hierarchical structures – typical of bureaucracies – are designed to reduce internal complexity by providing predefined rules of membership, channels of information flow and supervision mechanisms. However, as issues to be addressed become more complex and organisations grow, the effectiveness of hierarchical structures wanes – primarily due to absence of adequate resources coupled with constraints on information exchanges. Two questions are particularly relevant for the discussion on the future of the cyber security community: 1) how is it possible to achieve the desired policy outcomes and with what constellations of actors, and 2) how are policy outcomes are influenced by actors' roles and network structures.

Questions: *What are examples of methods applied by different countries and organisations?*
What lessons can we draw from those experiences?

Impulse givers **Enrico Calandro**, Research ICT Africa, Cape Town
Raul Zambrano, Global lead and Policy Adviser, Access to Information and e-governance, Bureau for Development Policy, UNDP, New York (tbc)

15:45 – 16:00 **Coffee break**

16.00 – 17.00 **HOW DO WE GET THERE?**

Based on the discussions throughout the day, in this session we will aim to assess possible ways forward for the cyber community. What conclusions can we draw for bringing different communities together? What resources are still required?

Impulse givers **Adriane LaPointe**, Senior Policy Advisor, Office of the Coordinator for Cyber Issues, U.S. Department of State, Washington, D.C.

Heli Tiirmaa-Klaar, Head, Cyber Policy Coordination, European External Action Service, Brussels