Cyber Capacity Building
in Ten Points

This note is based on deliberations during the international conference on cyber capacity building hosted by the EU Institute for Security Studies (13-14 March 2014, Paris) that brought together policy makers and practitioners from various communities in order to share their experiences and discuss ways forward for cyber capacity building.

Instead of traditional conference report, this note presents major take-away points. As such, this document aspires to be used as a reference and a quick introduction for anyone who is or wishes to get involved in debates about cyber capacity building.

The views expressed here do not represent the official position of the EU Institute for Security Studies, nor any other European Union institution.

Patryk Pawlak
Senior Analyst
European Union Institute for Security Studies

Ten major take-away points

1. **Cyber capacity building is not a sprint. It is a marathon.**
2. **Cyber capacity building needs a common language.**
3. **Cyber capacity building is not only about security.**
   It impacts social and economic development worldwide.
4. **Cyber capacity building challenges are not the same for everyone.**
5. **Cyber capacity building priorities are not the same for everyone.**
6. **One size does not fit all. But it fits most.**
7. **Cyber capacity building requires international coordination.**
8. **Cyber capacity building requires stakeholders' cooperation.**
9. **Cyber capacity building is not a priority. But it should be.**
10. **It is time to move from needs to delivery.**

1. Cyber capacity building is not a sprint. It is a marathon

- The importance of capacity building in cyberspace is increasingly acknowledged by governments, international organisations and the private sector. While the pressure on everyone to **deliver results** is mounting, the focus on **quick gains** in short period should not overshadow the **ultimate goal:** providing resilient ICT domain that supports economic and social progress.
- The cyber capacity building efforts need to be designed as a **chain process** whereby small initiatives contribute to a larger project. This should be reflected accordingly in the assessment of ongoing efforts and in the planning of future initiatives.

2. Cyber capacity building needs a common language

- The increasing reliance on ICT in all spheres of life will completely transform our societies and our systems of governance**. Effective mainstreaming** of cyber issues into debates in other policy areas – including development, agriculture, energy, transportation – needs to be part of the debate.

- The discussion about cyber capacity building is **too often underpinned by misconceptions** about the process, actors involved and respective responsibilities. This is especially so with regard to the (in)ability to differentiate between cybersecurity, cyber crime and cyber defence. References to cybersecurity are often politically loaded which, in conjunction with the existing misconceptions, results in problems in the implementation of concrete projects.
- The results **of capacity building** efforts in other areas are mixed, with the question of how to ensure sustainability posing the biggest challenge. Therefore, clear strategies for addressing the issue of sustainability need to be incorporated in any capacity building efforts.
- Cybersecurity needs to be **demystified.** It is not about military cooperation but about **fighting crime, building resilience** and **creating a safe environment** in which individuals and nations can develop.

3. Cyber capacity building is not only about security. It impacts on social and economic development worldwide

- An increasing number of countries rely on the internet and ICT for governance and delivery of services (e-government, e-health, e-education, online banking, etc.). Therefore, any efforts to improve security in cyberspace need to be addressed in the context of their impact on **good governance** (i.e. transparency, legitimacy and accountability of government authorities and officials), **human rights** (i.e. right to privacy) or **economic freedom** (i.e. online transactions, counter-corruption).
- The discussion on the **post-2015 Millennium Development Goals** presents a unique opportunity to link the debate to cybersecurity/ICT and their impact on economic and social development.

4. Cyber capacity building challenges are not the same for everyone

- **Challenges defined by donors**: developing scalable models for capacity building; defining a strategic framework for capacity building that would unify multiple projects and initiatives; engaging ministers and leaders at top and mid-levels is an important task for all stakeholders; coordinating with right partners at national and local level.
- **Challenges defined by beneficiaries**: dealing with harmonisation despite regional complexities; activating leaders on realities of cybercrime; moving from plans to implementation; setting clear priorities: fighting war, feeding people, or fighting crime?

5. Cyber capacity building priorities are not the same for everyone

- **A wish-list of donors:** increasing access to internet; improving the ability to utilise the web; developing local content; promoting the model of open and secure internet; developing reliable and trusted infrastructure; developing right skills and knowledge; putting in place legal frameworks that safeguard the rule of law and human rights.
- **A wish-list of beneficiaries:** tailored programmes; training, skills and knowledge building; criminal justice; provision of equipment.

6. One size does not fit all. But it fits most

Designing a **framework** for capacity building in a country or a region requires the recognition of the **specificities of a given context** (i.e. cultural, political and social heritage) and needs to ensure **local ownership**. While individual components of existing frameworks are case specific, the overall approach and objectives can be replicated. For instance, even though responsibilities can be assigned differently depending on the country in question, functions often remain similar.

- **National cybersecurity strategies** are a crucial component of capacity building. While their elements and principles are usually similar, the level of their **implementation** varies. The **clarity of objectives** (i.e. economic and social development, fight against the cybercrime, etc.) and **the mandate** for each organisation is critical to apportioning who should do what.
- The challenge of designing **policies** and drafting **legislation** is solvable but stakeholders need to take responsibility (i.e. the state for law enforcement and public safety, industry for network reliability). Each type of stakeholder (technical, managerial, political) reacts to different types of message and different sorts of carrots and sticks. A strategy has to be **flexible** enough to ensure the implementation model reflecting these different incentives.

7. Cyber capacity building requires international coordination

- Even though it is not yet clear how a more efficient **division of labour** could be ensured, **international cooperation** is imperative for two main reasons: a) cyber-related **threats** know no borders; b) the scope of investment needed to take full advantage of the **opportunities** offered by ICT exceeds the capacities of any single nation.
- In their search for a model of international cooperation, both donor and beneficiary communities should **focus** their efforts on identifying **good and bad practices**, **sharing information** about the capacity building efforts and coordinating of **resources.**
- For the exchange of **promising practice** to be effective, peers have to be at a relatively similar stage of implementation. It is difficult for one country to derive and extract useful practices from a much more advanced country. Guidance and promising practice must therefore be rooted in an understanding of the progress to date of any country.
- **Sharing information** between different actors (including within and between governments) is important in order to identify needs, success stories and failures, and to better understand specific conditions that influence an outcome. In that respect, a better exchange of information between regional and international organisations (in particular the World Bank and the United Nations agencies) on their respective capacity building efforts would be very welcome.
- International competition for **resources** for capacity building needs to take place in a productive way. While competition cannot be avoided, a more efficient use of resources can be ensured through monitoring where the resources are invested. Governments in partner countries should be encouraged to provide a platform that would facilitate the monitoring of where resources are allocated.
- **Regional organisations** like the Organisation of American States, the African Union Commission, the ASEAN or the Council of Europe might be good channels for capacity building efforts. However, they each have their own **limitations** prescribed by the extent to which they share **cultural values**, **language** regimes (e.g. three language groups in Africa as opposed to primarily Spanish-speaking countries in Latin America), **legal frameworks** or **mandate** (e.g. the African Union Commission implements its measures through five Regional Economic Communities – COMESA, IGAD, ECOWAS, SADC and ECCAS).

8. Cyber capacity building requires stakeholders' cooperation

- There are different ways to **benefit** from stakeholder cooperation: a) it **energises**, ensures **better capacity** and **results** in holistic outcomes with a greater perceived **legitimacy** (e.g. in Nigeria, Kenya, Ghana, Pakistan); b) it helps promote **good governance** (e.g. Sri Lanka CERT and Central Bank Payment System).
- For a multistakeholder approach to yield **results,** the main objective – around which specific initiatives will be developed - needs to be **clear** and the entire community of stakeholders brought together (including government, industry, community participation, local councils, and state governments).

- The **private sector** plays a crucial role in awareness raising by helping governments understand the importance of cyber issues (e.g. banks in their relations with ministries of finance, telecommunication companies in their relations with ministries of telecommunication, etc.). In order to form a productive, trusted working relationship, the private sector needs to better explain its decision-making process to governments.
- The role of **civil society organisations** (e.g. NGOs, think tanks or trade unions) is important in identifying the **needs** and **implications** of capacity building efforts, including the social and economic impact of internet roll out, potential abuses of workers (e.g. in cyber farms) or illegal activities.
- **Incident reporting** is a major challenge and some countries have begun to consider the imposition of positive obligations on the private sector (e.g. in Kenya). One way to counter the fear of reputational damage is the development of non-attributive reporting mechanisms (e.g. via reporting to a trusted third party). The lack of trust between actors involved and unclear mechanisms on how (and to whom) reports must be sent complicate the issue further.
- **Elements required to succeed**: leadership, inclusive process, diversity in approach, working towards common goals, tangible and intangible benefits.

9. Cyber capacity building is not a priority. But it should be.

- For many actors cybersecurity is not a political priority because there are more **pressing issues** (food security, sanitation, crime, infrastructure development, etc.). This is not because there are no risks but because the **risks are not visible**: incidents occur but they are not discussed publically.
- **Cybersecurity** is valued where there is a broad application of technology in the public sector and where the contribution of science and technology is valued. When governments do not have an **appreciation of the risk**, IT and capacity building is dropped from the agenda. The uptake of IT in some countries (e.g. Senegal, Kenya, Morocco, Vietnam and the Philippines) is significant but is not matched by similar levels of investment in developing security.

10. It is time to move from needs to delivery

- Capacity building programmes have to **evolve** in order to adjust objectives to the changing context, needs and maturity of the cyber policy framework of a specific actor (i.e. focus on awareness raising, building CERT/CSIRT, development of a strategy, industrial control systems, and exercises).
- The definition of the outcome at the start might result in the loss of **capacity to innovate**. While trials and errors need to be part of that effort, learning mechanisms need to be part of the process. Political leaders also need to **empower** individuals who take decisions.
- Conditions for **success**: a strategy, qualified staff, flexibility, sufficient resources, building networks, sharing experiences, international cooperation.
- **Priorities** to make the biggest change in 2014:
  a) Foster more global leadership and a sense of accountability for everyone;
  b) Develop sustainable knowledge-sharing mechanisms;
  c) Utilise big data and analytics to have better insight into incidents;
  d) Intensify efforts to create strategies that can mobilise all actors;
  e) Keep ears open to different views and perspectives;
  f) Clearly set out roles and responsibilities for stakeholders;
  g) Develop cybersecurity ‘safeguards’ for development projects.