INTERNATIONAL CONFERENCE ON

IDENTIFYING THE NEEDS OF NETWORKS ENHANCING THE ECONOMY, DEVELOPMENT AND SECURITY (NEEDS)

CYBER NEEDS AND DEVELOPMENT

BRUSSELS, 23-24 FEBRUARY 2015

BACKGROUND NOTE

The rapid spread of information and communication technologies (ICT) offers significant economic and human development opportunities to mankind. These are, however, accompanied by potential vulnerabilities and serious risks. Our increasing reliance on ICT in all aspects of daily life has created a new environment for criminal activities, such as massive online fraud schemes, computer intrusions, threats to critical information infrastructure networks, dissemination of terrorist propaganda, and other negative phenomena that can jeopardise or even negate the benefits deriving from the use of ICT. No country is immune to these threats and international cooperation is crucial for any serious attempt to mitigate these weaknesses. Developing countries – with limited means to address challenges posed by malicious cyber activities – are particularly vulnerable, especially as they are experiencing exponential growth in the number of internet users.

The European Commission's Directorate General for International Cooperation and Development, together with the European Institute for Security Studies, will co-host an international conference on 23-24 February 2015 in Brussels with the aim to contribute to the identification of cyber capacity building needs in developing countries. It is designed to generate a better understanding of the actions required to strengthen international Networks Enhancing the Economy, Development and Security (NEEDS). NEEDS are existing formal and informal mechanisms and structures of cooperation between public and private actors, at both policy and operational levels, which are designed to leverage cyberspace as a means for advancing economic growth, development and security. In that sense, NEEDS is an umbrella term used to highlight the necessity for cooperation between different communities with stakes in the future of cyberspace.

Whereas several such networks have been active for many years now and established a solid ground for national and international cooperation on cyberspace1, the scope of the challenge and its evolving nature require constant monitoring and more effective and targeted engagement. One of the key challenges in that respect is the identification of 'cyber needs of NEEDS'. In an effort to support ongoing processes and streamline future actions, the conference will take stock of current initiatives through discussions focused on cyber needs in three policy areas: cybercrime and justice, protection and resilience of critical infrastructure, and resilient e-development. We will explore these topics in three working sessions devoted to legal and regulatory development (i.e. legislative processes, oversight), structural and organisational development (i.e. distribution of competences, management structures, organisation of relationships between various actors), and human resources and technical expertise (i.e. skills and access to knowledge, training).

1 For instance, the Convention on Cybercrime has created a very robust community of law enforcement and justice experts. Similarly; many regional organisations have actively dealt with the different operational elements of cyber policy by, for example, establishing national Computer Emergency Response Teams or developing a national cybersecurity strategy.

1 ENHANCING ECONOMIC GROWTH, DEVELOPMENT AND SECURITY

The development community has long recognised that the spread of the internet has created new ways to empower people by providing them with access to services such as banking, health or information, which would otherwise be unavailable. As world leaders accelerate efforts to finalise a new catalogue of post-2015 development objectives, global internet usage continues to expand: almost three billion people now use online platforms to communicate, work, learn or access government services. It is not surprising, therefore, that the development community is pondering how to better leverage the benefits of the internet.

This exercise, however, will be futile if it is not accompanied by a serious discussion about the need to address vulnerabilities stemming from the proliferation of ICT infrastructure and internet applications. With the number of internet-connected devices expected to reach 15 billion in 2015, it is impossible to ignore the fact that the benefits of the internet on human development are unlikely to materialise without a secure and safe digital environment. As highlighted by the World Development Report 2014, 'the consequences of mismanaged risks may destroy lives, assets, trust, and social stability. And it is often the poor who are hit the hardest' (World Bank, 2014). The challenge is even more pressing given that the fastest growing numbers of internet users are in developing countries – in particular in Africa and Asia. Consumed by more pressing issues directly linked to social and economic development, many of those countries see the 'digital wave' as an opportunity without paying sufficient attention to the associated risks. Even though awareness is slowly increasing in a certain number of countries, they are often hobbled by limited resources or a lack of expertise. Consequently, capacity building – in addition to market mechanisms – has become a key approach which endeavours to ensure a minimum level of cybersecurity across the globe.

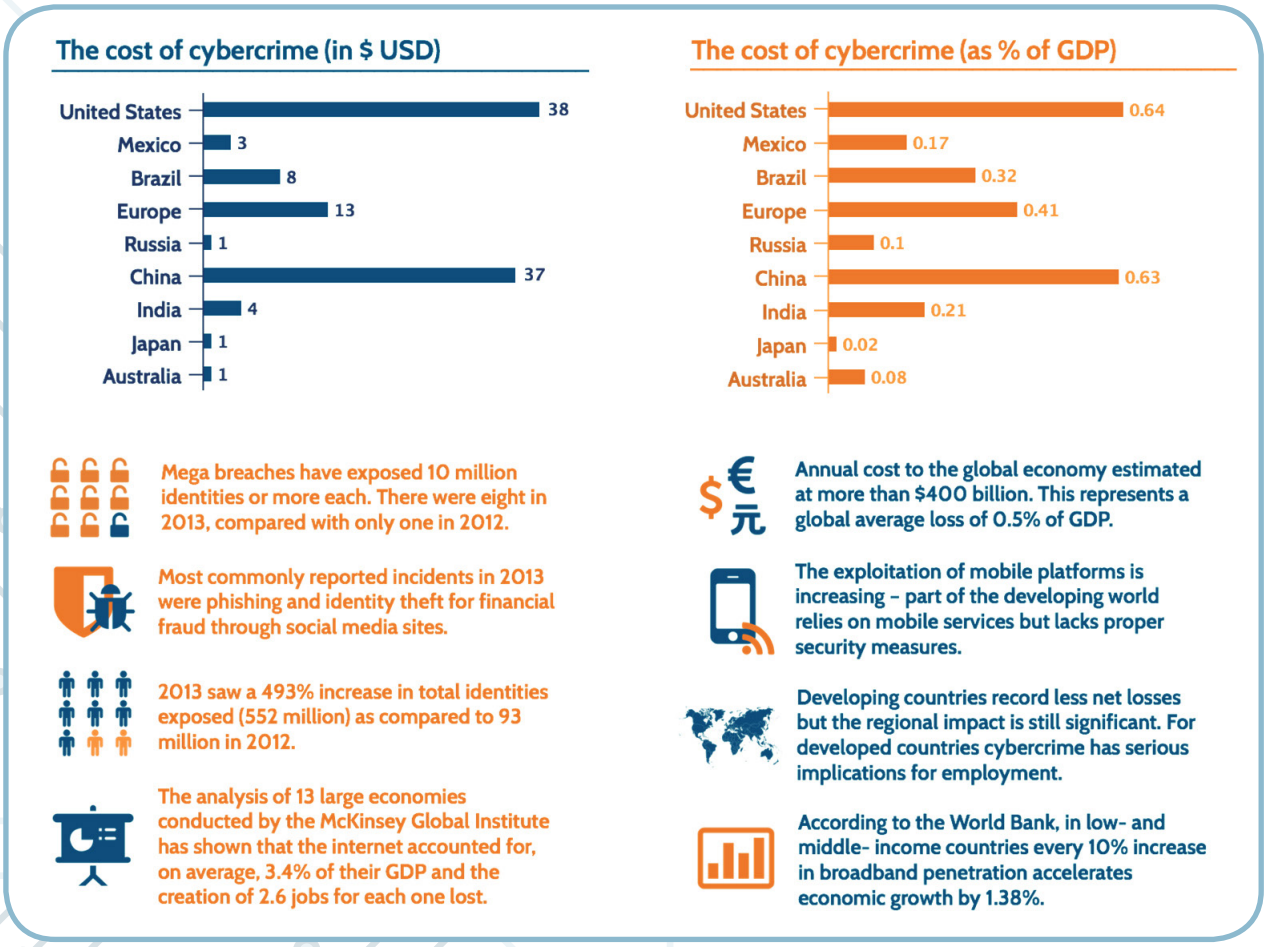

Figure 1. Cybercrime and development

2 ASSESSING CYBER NEEDS: STATE OF THE ART

The idea of mapping the ongoing cyber-related efforts and their effectiveness has increasingly attracted the attention of scholars and private actors (Annex I). The Network Readiness Index, published annually by the World Economic Forum, is one of the most comprehensive studies measuring access to ICT and its social and economic impacts. The existing body of research on the role of internet and ICTs is being progressively supplemented by cybersecurity-oriented projects ranging from qualitative mapping exercises aimed at taking stock of ongoing initiatives to more quantitative approaches proposing 'cyber maturity' or 'cyber readiness' indexes.

Many of these studies take the form of a mapping exercise whereby authors aim to provide an overview of the ongoing initiatives in individual countries and, on that basis, draw conclusions about the stage reached with regard to cybersecurity policy (UNIDIR, 2013). Some studies go further: in addition to providing an overview of ongoing efforts, they include an analysis of major security trends and challenges (OAS and Symantec, 2013). On the other end of the spectrum are projects that aim to measure and rank individual countries with regard to their level of cybersecurity development. For instance, the Cyber Readiness Index evaluates the commitment to securing the cyber infrastructure and services in order to highlight the negative impact of cyber insecurity on economic growth (Hathaway, 2013). Researchers from the Global Cyber Security Capacity Centre have put forward a Cyber Security Capability Maturity Model whereby countries are ranked on a scale ranging from those with only *ad hoc* levels of capacity to those with a strategic approach and an ability to adapt to environmental considerations (Global Cyber Security Capacity Centre, 2014).

Simultaneously, a number of ICT companies and consultancy firms have turned their attention to identifying drivers in enhancing cybersecurity, measuring policy performance (Kleiner et al., 2014), and more broadly the role of the internet in stimulating economic development (McKinsey Global Institute, 2011). These efforts are now being matched by intergovernmental processes. The Inter-American Development Bank, in partnership with the Organisation of American States, is preparing a study focusing on challenges and needs in Latin America and the Caribbean. In addition, the ITU and ABI Research are jointly working on the Global Cybersecurity Index.

Even though such studies set the tone of the discussion about cyber-related needs and the potential orientation for capacity building efforts, they cannot replace proper needs assessment processes commonly used by the development community (UNDP, 2009). Developing instruments to assess needs specific to cyberspace plays an important role in ensuring that challenges are prioritised and addressed in an effective and efficient way. Based on the overview of available indexes and maturity models and information drawn from development literature, it is possible to identify three main axes of needs assessment for cyber policies.

2.1 LEGAL AND REGULATORY NEEDS

An adequate regulatory and legal framework is considered to be the main building block in developing cyber capacities. It is required in order to impose certain obligations, assign responsibilities and sanction certain type of behaviour. Numerous initiatives to improve legal capacities when dealing with cybercrime, adopt a national cybersecurity strategy or protect critical national infrastructure have already been completed or are underway. There is, however, a consensus that the biggest challenge remains their successful implementation. In addition, there is a risk that several frameworks developed regionally might jeopardise the efforts towards interoperability and the harmonisation of practices at an international level. Numerous countries, including in the EU, have adopted the Convention on Cybercrime (known also as the "Budapest Convention") to address this challenge given that it is the only binding international

instrument on this issue and serves as a model for developing comprehensive national cybercrime legislation, while it also provides an effective framework for international cooperation in this field. Finally, with different levels of development around the world and technology fast-evolving, there is a need to ensure that the applicable legal frameworks are sufficient to deal with new developments.

POTENTIAL TRIGGER QUESTIONS

- Is there a comprehensive cybersecurity strategy and/or a legal/policy framework to deal with cybercrime or ensure the security of critical national infrastructure? If yes, *what do you need* to make implement them effectively, also in terms of international cooperation? If not, what are the obstacles you face and *what do you need* to overcome them?

- How does the existing legislation improve the capacities of institutions, companies and individuals to innovate and exercise their rights? *What do you need* to make the legal framework work for the benefit of the citizens? *What do you need* to minimise the digital security risks to companies or individuals?

- Is there a framework for certification or implementation of internationally recognised cybersecurity standards in the public sector or among critical infrastructure operators? If yes, *do you need* to improve the performance of this framework? If not, *what do you need* to set it up?

2.2 INSTITUTIONAL AND ORGANISATIONAL NEEDS

Putting laws into practice, and implementing and enforcing policies requires well-functioning and coordinated institutions and procedures. This is particularly important in two cases: i) when implementing a national cybersecurity strategy, and ii) for preventing, detecting and responding to potential cyber attacks (i.e. a national level CERT or CSIRT). As countries adopt different models in line with their cultural and political backgrounds (i.e. some have set up such bodies in the ministries of defence, while others in the ministries of telecommunications), it is essential to gain a thorough understanding of each specific domestic context. Given their importance in any attempt to increase cyber resilience, management structures, as well as coordination mechanisms and other institutional factors must also be explored. Elements such as leadership, the management of relationships (i.e. between public and private actors), and accountability mechanisms are often decisive in ensuring that a project or undertaking is sustainable.

POTENTIAL TRIGGER QUESTIONS

- Is there a national entity in charge of preventing, detecting and responding to potential cyber attacks and/or a body responsible for the implementation of a national cybersecurity strategy? *Do you need* one and *what do you need* to make it happen? *What do you need* to identify and respond more effectively to potential risks?

- How does your organisation fit within the broader architecture in your country? Do you think your organisation is implementing its mandate in the best way possible? *What do you need* to do better?

- Are the responsibilities among main stakeholders clearly assigned and understood? *What do you need* to make different agencies work better together? *What do you need* from the private sector and what does it need from you? What is needed to satisfy both sides?

2.3 HUMAN RESOURCES AND TECHNICAL EXPERTISE

With the internet and ICT technologies becoming an integral part of most human activities, the development of human capacities to deal with digital security risks across various policy areas is essential. This means developing skills, raising awareness, generating knowledge, and, ultimately, retaining talented staff. As all actors struggle to generate enough cyber manpower, the challenge is to develop adequate technological expertise to detect and respond to cyber attacks and build confidence and trust in cyberspace among citizens.

POTENTIAL TRIGGER QUESTIONS

- Is homegrown expertise available? What are the main obstacles to generating a qualified work force? *What do you need* to overcome them?

- What is the level of cyber competencies amongst the general population? Are there education and training programmes available? *What do you need* to improve the overall level of knowledge among managers and employees at all levels?

- What is the level of competence within your own organisation? *What do you need* to make better use of existing resources, as well as generate new ones?

- Are there established channels of communication with the wider public on cyber-related issues in order to strengthen their confidence on the internet? *What do you need* to communicate and better promote a cybersecurity mindset?

3 ADDRESSING NEEDS WITH CAPACITY BUILDING

In light of the divergence in the progress made between the different parts of the world, capacity building in cyberspace has increasingly dominated international cooperation agendas in this field. Even though the number of initiatives is growing, levels of coordination – both in terms of objectives and implementation – could be significantly improved. Overall, there is also a growing imbalance between increasing demand and limited supply – the skills and knowledge of leading cybersecurity practices are simply not being shared fast and wide enough.

Part of the problem stems from the fact that there is no systematic international effort aimed at assessing cyber needs – even where such assessments are undertaken in specific policy areas, they are hardly ever shared among policy communities. Answering this challenge requires acknowledging that development objectives and risks related to the digital environment are effectively two sides of the same coin, and so need to be addressed in a comprehensive and coordinated manner. This also means that different communities – diplomats, security experts, law enforcement and development officials – need to work together more effectively.

The need for cross-fertilisation between disciplines is even more important when potential risks are expanded from attacks on individuals and companies (i.e. phishing, mobile spoofing) to more sophisticated threats against societies at large (i.e. attacks on critical infrastructure, such as energy and water networks) or governments (i.e. data breaches, DDoS attacks). Three policy areas are particularly useful testing grounds for building genuine and effective networks enhancing the economy, development and security.

3.1 CYBERCRIME AND JUSTICE

Cybercrime is a term which covers criminal acts specific to the internet, such as attacks against information systems, and different methods of spreading malware. Computers are also used as criminal tools to commit more traditional crimes, such as fraud or the dissemination of illegal content. The scale of the problem poses a threat to law enforcement response capability. As other forms of crime (i.e trafficking, money laundering, etc.) increasingly gain a 'cyber' dimension, it is becoming ever more difficult for law enforcement and judicial bodies to effectively address those challenges without tackling a 'cyber' component. At the same time, the multi-jurisdictional nature of cybercrime and the ways to address it adds further layers complexity with regard to how it is investigated, and eventually punished by the authorities. Certain instruments and tools are already available and legislative reforms have been widely initiated or completed in recent years to address this complex issue. However, the strengthening of institutional capacities so as to ensure the completion of legal reforms (and the application of legislation to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving electronic evidence) appears to be a persistent challenge. Developing the necessary knowledge base and relevant training programmes for the law enforcement and criminal justice authorities is therefore key.

3.2 CRITICAL INFRASTRUCTURE PROTECTION

The smooth and secure functioning of critical infrastructure (i.e. power plants, oil refineries or transportation systems) is essential for economic, social and human development. With countries increasingly reliant on the use of ICT to optimise the operation of ports, energy grids or manufacturing facilities, it is paramount to

identify the vulnerabilities of these highly inter-linked communication networks and information systems which could be exploited for political reasons or financial gains. Critical infrastructure encompasses large complexes controlled and monitored by Industrial Control Systems (ICS), including SCADA systems (Supervisory Control and Data Acquisition). In an effort to reduce costs, many ICS products use commercial off-the-shelf software and apply standard embedded systems platforms. The downside of such a solution, however, is that ICS are vulnerable to network-based attacks.

While the principal responsibility for security falls on individual countries, the international community cannot ignore the negative internal and external implications of potential attacks on critical infrastructure in developing parts of the world. Even though the probability of large-scale attacks is still considered relatively low, the magnitude of potential consequences (i.e. from an attack on a nuclear power plant) means that all governments have a stake in the matter. The capacity of many developing countries to monitor and manage such incidents in cyberspace is, for now, rather limited but can be improved with investment in technological and organisational measures, including the setting up Computer Emergency Response Teams (CERT), acquiring the right equipment and receiving specialised training. Effective cybersecurity capacity building entails, *inter alia*, a functioning national CERT which feeds information to law enforcement agencies and acts as interface between government bodies and the private sector.

3.3 RESILIENT E-DEVELOPMENT

The development of e-government and the application of ICT to various areas of human activity are believed to be important instruments in the pursuit of sustainable development. Governments across the world are devoting substantial resources to upgrading their infrastructure, telecommunication systems or energy networks using elements of ICT. This makes it increasingly difficult to treat cybersecurity as a distinct policy area. The transformational power of ICT to deliver new solutions to traditional development challenges can be easily undermined if risks associated with these new technologies – mobile and internet tools in particular – are not adequately managed. Disruptions may have disastrous consequences for the country at hand and the need to ensure robustness against cyber-attacks is therefore of primary importance. At the same time, the need to create the right policy environment for ICT roll-outs and reforms in specific policy areas empowering citizens and businesses alike must also be addressed.

CONCLUSIONS

Networked problems require networked solutions. Several national, regional and global initiatives are already underway. But as technology evolves and makes advances into new areas of human activity the challenge for international community is to stay ahead of a curve – or at least not too far behind.

It takes a network to beat a network. Hence, cooperation between different policy communities is not an option but a necessity. True, the technological, legal, institutional and cultural differences between the countries of the world indeed pose a challenge – but they can be overcome if we gain a better understanding each other's situation and needs.

POTENTIAL TRIGGER QUESTIONS

- *What do we need* to improve cooperation between different policy communities?
- *What do we need* to ensure that the supply and demand sides of cyber capacity building are better aligned?
- *What do we need* to build effective and sustainable international partnerships?

ANNEX I

Overview of existing maturity models and readiness indexes

MODEL	ELEMENTS/INDICATORS TAKEN INTO ACCOUNT
NETWORK READINESS INDEX (World Economic Forum)	• Political and regulatory environment, business and innovation environment • Infrastructure and digital content, affordability, and skills • Individual, business and government usages • Economic and social impacts
CYBER READINESS INDEX (Hathaway, 2013)	• Articulation and publication of a national cyber security strategy • Operational Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) • Demonstrated commitment to fight cybercrime • Information sharing mechanisms in place • Investment in cybersecurity, basic and applied research, and broader cybersecurity initiatives
PREDICTING CYBERSECURITY PERFORMANCE (Microsoft, 2014)	• Identification of relations between CCM (computer cleans per mille – thousand) and other national indicators or factors like gross income per capita, rule of law, demographic instability or Facebook usage.
CYBER SECURITY CAPABILITY MATURITY MODEL (Global Cyber Security Capacity Centre, 2014)	• Cybersecurity policy and strategy • Cyber culture and society • Cybersecurity education, training and skills • Legal and regulatory framework • Organisations, technologies and standards
REGIONAL CYBER MATURITY (Australian Strategic Policy Institute, 2014)	• Organisational structures • Existing legislation/regulation • International engagement • Computer Emergency Response Team (CERTs) • Military application • Government-business dialogue • Digital economy • Public awareness • Internet penetration
GLOBAL CYBERSECURITY INDEX (ITU&ABI Research, 2014)	• Legal • Technical • Organisational • Capacity building • Cooperation

REFERENCES

- Australian Strategic Policy Institute, *Cyber Maturity in the Asia-Pacific Region 2014*, Canberra, 2014.
- Global Cyber Security Capacity Centre, *Cyber Security Capability Maturity Model*, Oxford, 2014.
- Kleiner, A., Nicholas, P. and Sullivan, K., *Linking cybersecurity policy and performance*, special edition of the Microsoft Security Intelligence Report, 2014.
- McKinsey Global Institute, Internet matters: the Net's sweeping impact on growth, jobs, and prosperity, May 2011.
- Organisation of American States and Symantec, *Latin American and Caribbean Cyber Security Trends*, Washington, D.C., 2014.
- UNDP, *Frequently Asked Questions. The UNDP capacity assessment methodology*, Capacity Development Group, June 2009.
- World Bank, *Risk and opportunity. Managing risk for development*, World Development Report 2014, Washington, D.C., 2014.