ISSUE

REPORT Nº 21 – December 2014

Riding the digital wave

The impact of cyber capacity building on human development

EDITED BY
Patryk Pawlak

Reports

ISS European Union Institute for Security Studies

EU Institute for Security Studies

100, avenue de Suffren

75015 Paris

http://www.iss.europa.eu

Director: Antonio Missiroli

ISBN 978-92-9198-250-9

ISSN 2363-264X

QN-AF-14-004-EN-N

Doi:10.2815/43313

Published by the EU Institute for Security Studies and printed in Condé-sur-Noireau (France) by Corlet Imprimeur.

Graphic design by Metropolis, Lisbon.

Maps in annex: Léonie Schlosser.

Cover photograph: Oxfam/Sven Torfinn.

CONTENTS

FOREWORD

When the member states endorsed the EU Cybersecurity Strategy in June 2013, they expressed a wish for the Union to take a more active role in this highly dynamic, fast-moving policy area. Ever since, issues linked to the security of cyberspace have featured prominently in the media – in relation either to fresh attacks on government websites and services or to exciting opportunities created by new technologies. The importance of a flexible, open and secure digital environment for economic growth has also been recognised by the new President of the European Commission, Jean-Claude Juncker, who made the completion of a European digital single market one of his policy priorities.

As a result, over the last year various Commission departments and the European External Action Service have worked together to project the EU's vision for cyberspace and advance its policy preferences. Thanks to new financing possibilities offered by the Instrument contributing to Stability and Peace (IcSP), the EU has established itself as one of the key players in cyber capacity building, in particular with regard to the fight against cybercrime. And the EUISS Cyber Task Force, established in March 2013, has been particularly helpful in bringing together stakeholders from all over the world.

This report offers a valuable contribution to shaping the EU's posture on capacity building. By promoting a development-focused approach to the issue, it provides a valuable alternative to the predominantly threat-oriented narrative about cybersecurity. The authors address security not as an end in itself but rather as a means towards social, economic and political development. Consequently, they seek to build bridges between different policy communities. As noted on numerous instances in these pages, such a comprehensive and integrated approach to cyber capacity building is instrumental to ensuring the sustainability and the effectiveness of current and future initiatives in this domain.

Joëlle Jenny
Director for Security Policy
and Conflict Prevention
European External Action Service

Antonio Missiroli
Director
EU Institute for Security Studies

December 2014

INTRODUCTION

Patryk Pawlak

As world leaders accelerate efforts to finalise a new catalogue of post-2015 development objectives, global internet usage continues to expand: almost three billion of the world's population now uses 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 stemming from the use of Information and Communication Technologies (ICT). This exercise, however, will be futile if it is not accompanied by a serious discussion about the need to address risks posed by the proliferation of ICT infrastructure and internet applications for sustainable development.

In this context, as one of the biggest donors and an important player on the global stage, the European Union is committed to ensuring that building resilient capacities to mitigate digital security risks around the world also contributes to economic and social development, as well as strengthening the international rule-based order that supports human rights and the rule of law. The EU is a staunch supporter of the Council of Europe Convention on Cybercrime that not only fosters cooperation in the fight against cybercrime but at the same time promotes a human rights regime established within the Council of Europe system. In the framework of the Instrument contributing to Stability and Peace (IcSP) the EU has committed approximately €21.5 million for the period 2014-2017 to fight cybercrime and improve cybersecurity in other parts of the world.

The challenge is even more pressing given that the fastest growth in the number of internet users is taking place in developing countries – in Africa and Asia in particular. Consumed by more pressing issues directly linked to social and economic development, most of those countries see the 'digital wave' as an opportunity without paying sufficient attention to the associated risks. Even though awareness is slowly building up in a certain number of countries, they are often hobbled by limited resources or lack of expertise. Consequently, capacity building – in addition to market mechanisms – has become a key instrument at the disposal of the donor community through which to ensure a minimum level of cybersecurity across the globe.

Cybersecurity in this report is understood as a way to empower individuals, communities and governments to achieve their developmental goals by reducing digital security risks stemming from access and use of Information and Communication Technologies. This report takes a broad view of risks which include not only those posed by either state or non-state actors to another state and its citizens (i.e. loss of data, attacks

on government websites), but also those resulting from a state's negligence or premeditated actions against its own citizens (i.e. surveillance programmes, content blocking). Such a definition results from our broader view of security not as a goal *per se* but rather as an enabler of political, social and economic transformation that may not always be identical to security objectives as defined by a state. Consequently, the term *cyber capacity building* is employed throughout the text as an umbrella concept for all types of activities (e.g. human resources development, institutional reform or organisational adaptations) that safeguard and promote the safe, secure and open use of cyberspace. Finally, in the absence of a universally accepted definition, in this report we refer to *cyberspace* as a digital environment (i.e. the internet, telecommunications networks or computer systems) that people use as means to achieve their social, economic or political goals.

About this report

A growing reliance on computer networks and internet-based applications in all areas of human activity (e.g. health, transportation, energy or education) makes it increasingly difficult to treat cybersecurity as a distinct policy area. Consequently, the number of stakeholders concerned with various dimensions of cybersecurity – government officials, executives in the private sector or civil society organisations – is expanding. Yet cybersecurity issues are too often viewed as purely technical and confined to the realm of IT departments, resulting in a limited general knowledge and awareness of the risks associated with internet connectivity. The purpose of this report is to change this perception and bridge cyber-related debates taking place separately in various policy communities.

The report features three main thematic strands highlighting different – albeit interlinked – axes of capacity building. The chapters by Patryk Pawlak and Neil Robinson focus on national capabilities and provide an overview of existing models and components of cyber capacity building: while the former pays particular attention to vertical distribution of responsibilities and tasks (i.e. between the national and international levels, between private sector and government), the latter focuses on horizontal blocks of capacity building (i.e. legal framework, institutional arrangements, etc.). The chapter by Maria Grazia Porcedda completes the picture with its insights on legal capacity building – as opposed to a narrowly defined cybercrime capacity building. Porcedda's analysis builds on the ongoing legal debates to demonstrate the importance of focusing on the rule of law and human rights as key factors in cyber capacity building and *de facto* connecting the fight against cybercrime to human development. Elena Kvochko in her chapter offers an overview of the perception and role of private sector actors. Based on research conducted by the World Economic Forum, she stresses the importance of cyber resilience for economic development and analyses the dynamics in the relations between public and private actors. The chapter by Enrico Calandro and Patryk Pawlak highlights the linkages

between development and cyber capacity building. The authors argue that ignoring the dimension of cybersecurity in the debate about development might result in a new type of cyber-related poverty and exclusion. Finally, the last chapter by Patryk Pawlak provides an overview of four distinct models of capacity building. It stresses the importance of an integrated approach to cyber capacity building as a solution to a growing demand and scarce resources.

The principal argument that this report aims to advance is that cyber capacity building is a developmental issue which requires cooperation among different policy communities in order to ensure that the gains achieved thanks to ICT deployment are not lost in the years to come. In that spirit, the following ten major guiding principles for cyber capacity building may be extrapolated from the analysis contained in individual chapters of this report:

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 on 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.

Acknowledgements

This report has substantially benefited from discussions and exchanges in the framework of the EUISS Task Force on Cyber Capacity Building. The members of the Task Force are extremely grateful to all government officials and experts who have participated in our discussions. In particular, they would like to thank Nayia Barmpaliou (European Commission), Laurent Bernat (OECD), Adriane LaPointe (US Department of State), Samia Melhem (World Bank), Heli Tiirmaa-Klaar (EEAS), and Raul Zambrano (UNDP) for their valuable insights throughout the duration of the Task Force. Our gratitude goes also to international partners who have supported our work from the very beginning: Belisario Contreras (OAS Secretariat), Matias Bertino Matondo (AU Secretariat), Budi Yuwono (ASEAN Secretariat) and Lasantha De Alwis (CTO). Their inputs provided inspiration and guidance for navigating in the complex space between the virtual and real worlds.

The authors would like to thank Nayia Barmpaliou, Lasantha De Alwis, Martyn Egan, Jens Kremer and Caroline Timon for comments on earlier drafts of the chapters. They

would also like to acknowledge their respective organisations – RAND Europe, World Economic Forum, Research ICT Africa and the SURVEILLE project at the European University Institute – for making this publication possible. At the EUISS, Beatrice Berton, Miruna Buros, Gergana Petkova and Catherine Sheahan provided invaluable assistance with the collection and organisation of data. Any error in analysis or interpretation is the sole responsibility of the authors.

I. DEVELOPING CAPACITIES IN CYBERSPACE

Patryk Pawlak

A secure and safe digital environment is a necessary condition for reaping the benefits of ubiquitous access to the internet and the positive impact it has on human development. With the number of internet-connected devices expected to reach 15 billion by 2015, addressing the threats posed by malicious cyber activities is a clearly of paramount importance. The exponential growth of Information and Communication Technologies (ICT) and the transformation that this has wrought in all aspects of everyday life has resulted in the emergence of a broad policy community relying on these technologies. *The Global Information Technology Report 2014* published by the World Economic Forum calls this the 'Internet of Everything' – an environment facilitated by the use of cloud and mobile computing, the growth of big data and development of the Internet of Things. A forecasting exercise conducted by Cisco – 'The Zettabyte Era' – suggests that the number of portable internet-connected devices will be nearly twice as high as the global population by 2018. Another report entitled *Cyberspace 2025*, released by Microsoft, estimates that in the next ten years the internet will be used by more than 91% of people living in developed countries and about 69% in developing ones.

But improved access to ICT and increasing reliance on the internet is a process that has been accompanied by growing risks and challenges, whose seriousness should not be underestimated. The explanation is twofold. The first aspect is related to a rapidly evolving threat landscape, in particular over the past five years. According to the 2014 *Symantec Internet Security Threat Report*, the total number of security breaches in 2013 was 62% greater than a year earlier, with more than 10 million identities exposed, which led the authors to dub 2013 'the Year of Mega Breach'. The nature of the attacks has also become more sophisticated. Lately, cyber attackers have become more aggressive in their exploitation of people's increasing reliance on online social networks and mobile devices. The ransomware scams – designed to encrypt a user's files and then demand payment of a ransom for the files to be unencrypted – that made their first appearance in 2012, grew by 500% over the course of 2013.

At the same time, many countries have only recently started to understand the extent to which cyberspace vulnerabilities and limited capacities prevent them from maximising the benefits stemming from the use of the internet as a platform for delivery of services like banking, healthcare or education. Symantec reports that every second, 18 adults are targeted by cybercrime, resulting in more than one-and-a-half million cybercrime victims each day. Europol estimates that victims of cybercrime lose around €290 billion each year worldwide, making internet crime more profitable than the global trade in marijuana, cocaine and heroin combined. A recent study by the Center for Strategic and International Studies released in June 2014 estimated the

cost of global cybercrime at USD 400 billion. In the light of this data it is clear that as countries move forward with their development programmes, they also need to pay attention to security aspects at different levels, including infrastructure, governance processes or personnel.

Consequently, the discussion about the investment in ICT is gradually being accompanied by cyber capacity-building efforts – as suggested, *inter alia*, in the 2013 UN report by the Group of Governmental Experts – aimed at improving the resilience and security of a broadly defined cyberspace. However, misconceptions about cybersecurity and what it means – and including the dimensions of cyber resilience, cybercrime and cyber defence – complicate the discussion between various policy communities (i.e. security and development but also trade and innovation) and make it more difficult to address cyber-related risks in a comprehensive manner. It would seem logical that, for instance, a project aiming at the development of a nuclear energy programme be accompanied by training on information and computer security for nuclear security practitioners (see Box 1), but such synergy is rarely to be found.

Comprehensive approach to cyber capacity building

The Agenda 21 – a non-binding action plan of the United Nations with regard to sustainable development adopted in Rio de Janeiro in 1992 – refers to capacity building as efforts at building the 'endogenous capacity' of a country to make informed policy choices. The United Nations Development Programme has elaborated on the concept by defining capacity building or development as a process by which societies, institutions or individuals increase their abilities to perform core functions, solve problems and work towards specific objectives in a sustainable manner. This process is primarily focused on three main elements: (i) human resources, (ii) organisational arrangements, and (iii) institutional and legal development.

The key challenge with regard to cyber capacity building is designing the process in such a way that it can be both effective and sustained over time. To achieve this objective it is crucial to reflect on how different stages of cyber capacity building relate to specific development objectives and how the distribution of responsibilities between individuals, governments and the international community can influence the process both in positive and negative ways (see Figure 1).

Box 1. Connecting the dots: IT and nuclear security

The International Atomic Energy Agency (IAEA) defines threats to nuclear security as unauthorised acts involving or directed at nuclear facilities or activities, and other intentional acts that could produce harmful consequences to persons, property, society or to the environment.

In response to potential threats to IT networks of energy facilities, the IAEA Department of Nuclear Security has initiated awareness training courses and advanced training courses in IT/Cyber Security. Main modules in the training programmes include computer security and access control, authentication and cryptography, computer security architecture, network security, intrusion detection and information recovery, network management practice.

The IT/Cyber Security Pilot Professional Development Courses (PDC) have been organised since 2012, bringing together participants from about 20 countries, including Ghana, Tanzania, South Africa, Russia, Thailand, Malaysia, Egypt, Iraq, Jordan, Kenya, Morocco, Nigeria and Ukraine. The European Union is also funding a Master Programme in Nuclear Security with the participation of Germany, the Netherlands, Austria, Norway, the UK and Greece.

The lessons from those engagements include: (a) the need to identify proper sources for educating professionals about cybersecurity and developing a common vocabulary (e.g. 'information security', 'IT/Cyber Security', 'Computer Security' or 'Cyber Security'); (b) identifying the right audience for the course (taking account of different levels of knowledge and familiarity with cyber issues) and the right set of issues (nuclear IT/Cyber security also includes digital safety and emergency systems).

Sources: IAEA (2011); G. Gluschke, presentation at EUISS workshop on capacity building, September 2014.

With regard to concrete security objectives the process of capacity building can be organised along four interlinked stages:

- *Prevention*: Even though cyberspace is characterised by systemic complexity, most of the risks associated with cyberspace are man-made. Therefore, understanding relations between men and technology is a crucial aspect. To that end, concrete capacity-building activities may be geared towards addressing the root causes of why individuals or groups are drawn to committing cybercrimes; raising awareness about the risks; reducing vulnerabilities, including those resulting from human error; and improving coordination of national policies (i.e. institutional arrangements, legislative measures, etc.).

- *Protection*: Due to the growing number of risks associated with cyberspace, protecting citizens and infrastructure from an attack or accident is another important element. Concrete actions may include cooperation between private and public actors towards reducing the impact of cyber-accidents, *inter alia* by creating a computer emergency response team (CERT), adopting adequate legislation, setting standards, developing models of cooperation, conducting risk assessments, joint exercises, etc.

- *Pursuit*: As an accident can be either a result of negligence or premeditated action, the attribution of the level of responsibility and potential sanctions needs to reflect that fact. Therefore, liability – including the possibility of criminal sanctions – is an important part of the discussion. In criminal cases – aimed at obtaining economic or otherwise motivated benefits – the efforts may focus on exchange of information, developing a common understanding of the threat, cooperation between authorities as well as adoption and implementation of international legal instruments.

- *Response*: Once a cyber event occurs, it is followed by actions to minimise and manage its negative consequences on the economic and social well-being of citizens, companies or institutions. Potential capacity-building activities in this area might include establishment of a CERT, appointing 24/7 contact points or improving the cooperation between governmental agencies, the private sector and other stakeholders.

Taking into account different levels of responsibility among stakeholders and varied modalities of engagement among them across these four areas, it is possible to identify three main axes of capacity building: (i) strengthening national capabilities; (ii) developing collective capability, and (iii) facilitating international cooperation and partnerships.

Strengthening national capabilities

Even though responsibilities for cyberspace are spread among many stakeholders (see the next section), the state still plays an important role in creating a legal and policy environment that helps to protect the benefits of an open and secure internet. As a matter of fact, law-making, law enforcement and defence are the exclusive prerogatives of the state. The state can perform this role either through government action (whenever it can act alone) or by providing the right incentives for other stakeholders (whenever it does not have the right resources). Such actions come in different forms: adopting a national security strategy and secondary legislation, building national computer emergency response teams, implementing legal and political reforms or entering into international agreements. This may explain why so many organisations have committed substantial resources to capacity-building projects aimed at law enforcement and judicial training, cybercrime or high-tech crime units, computer forensic capabilities, and IT security specialists.

Figure 1. Selected elements of comprehensive cyber capacity building

Developing collective capability

Bringing together different communities to address security challenges to cyberspace is not an easy task given the complexities of such a collective endeavour: different organisational missions and objectives (providing security versus making profit), working methods (law enforcement and public service versus efficiency) or various time frames (longer cycle for policy making or legislation versus the need to act instantly). The task is further complicated by the need to recognise different – albeit legitimate – approaches to dealing with cyber threats, mainly military, trade or law enforcement. The first step in overcoming those obstacles is for stakeholders to gain a clear understanding of their specific roles within this joint endeavour and of the framework within which these tasks can be implemented (see Box 2).

Box 2: Developing collective capability: public and private CERT communities

- **Regional network of CERTs in the Asia Pacific (APCERT)**

APCERT has as its objective to maintain a trusted network of computer security experts in the Asia Pacific region in order to improve the region's awareness and competency in relation to computer security incidents. Its activities include, among others, different initiatives focusing on: (i) enhancing Asia Pacific regional and international cooperation on information security; (ii) jointly developing measures to deal with large-scale or regional network security incidents; and (iii) assisting other CERTs and CSIRTS in the region to conduct efficient and effective computer emergency response.

- **Global network of CERTs: Forum of Incident Response and Security Teams (FIRST)**

Created in 1990, FIRST was born from the idea that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide-ranging attacks were the key issues for security and incident response teams. FIRST brings together a wide variety of security and incident response teams including product security teams from the government, commercial, and academic sectors. The Forum has been actively involved in capturing lessons from activities undertaken by members of the network, including publication of the best practice guide library on setting up a CERT.

- **Global network of governmental bodies on CIIP: Meridian Process**

The aim of the Meridian Process is to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP). It explores the benefits and opportunities of cooperation between governments and provides an opportunity to share best practices from around the world. Its open nature (it is open to all countries) allows the creation of a community of senior government policymakers in CIIP by fostering ongoing collaboration.

Sources: online sources (www.apcert.org, www.first.org, www.meridianprocess.org)

Facilitating international cooperation and partnerships

Coordinated international efforts are necessary to ensure a minimum level of cyber capacity across the globe. This often proves difficult given the competing objectives and

narratives about what needs to be protected, why and how. It is therefore essential to deepen international consensus and strengthen international cooperation with regard to prevention, protection, pursuit and response, including through international and regional organisations. As the examples from the ongoing projects demonstrate, different approaches are possible, including the designation of priority geographic areas (e.g. the European Union's focus on the Balkans), partnerships based on the level of threat (i.e. primarily cooperation between like-minded countries) or simply due to a country's or region's potential for becoming a hub – a regional champion – for developing bottom-up regional initiatives. It is also essential to recognise the differences in needs between developed and developing countries or even within the same region.

The need for closer coordination of efforts also stems from the fact that resources devoted to cyber-issues are still limited. Even though some countries are increasing their investment, most institutions lack sufficient funding for cyber-related programmes, which raises doubts as to whether they have a real capacity to maintain multiple and expanding relationships. Nonetheless, joint efforts at improving cyber capacities are underway. For instance, the Council of Europe Convention on Cybercrime provides a good basis for forging international cooperation frameworks around the issue of cybercrime.

Challenges of cyber capacity building

Cybersecurity capacity building is not immune to the dilemmas inherent in any other type of activity underpinning a donor-recipient relationship, and therefore learning from the capacity-building experiences of other communities might provide useful insights for cyber capacity building (see Box 3). Given different levels of development across the world, a collective capacity-building effort is of paramount importance in both preventing the emergence of safe havens and ensuring the benefits of ICT for development. There is no single 'good' model for securing cyberspace – therefore, the exchange of good (and bad) practices between individual countries and regional organisations may help streamline ongoing efforts. When discussing cyber capacity-building methodologies the lessons from other areas should not be ignored, including with regard to local ownership and the effectiveness of conditionality.

First, the donors' community needs to define a *strategic narrative* around the issue of cyber capacity building. For instance, the European Union and like-minded countries have made the protection of their core values (i.e. democratic principles, human rights, and the rule of law) and interests into a pillar of their cyber diplomacy. But with several other players simultaneously pursuing their own agendas, there is increasing confusion among the beneficiaries about the aims of similar projects and their added value. The absence of a clearly defined and unifying objective is also an obstacle to more efficient cooperation between donors. This does not imply that the imposition of one model on the whole international community would be a good idea but there

is clearly a need for a set of general guiding principles. Such a clear narrative – or narratives – would also help to allay any misunderstandings about intentions and the nature of the relationship between donors and beneficiaries (see Box 4).

Box 3. Learning from others: development community and capacity building

- **Choosing the right partner: GIZ and local government in Burkina Faso**

Identifying right partners is one of the most common challenges in any capacity building project. One of the initiatives implemented by GIZ – a German development agency – aimed at strengthening the capacity of the municipalities in Burkina Faso to deliver better services to citizens. A widespread agreement emerged on setting up a national training system with uniform quality standards for the administrative personnel. However, it became apparent that the ministry responsible for decentralisation was not in a position to manage this process and cooperation with another partner from the Ministry of Territorial Administration had to be established, which eventually helped to push the issue onto the political agenda.

- **Learning as a part of the culture of development cooperation: lessons from OECD ODA**

One of the key elements highlighted in a report entitled 'Evaluating Development Activities: 12 lessons from the OECD DAC' is the importance of a learning culture that encourages staff and management to flag, investigate and learn from success and failure. The reforms undertaken by the UK government in 2011 included the creation of an independent committee on development impact and strengthening evaluation capacities across the Department of International Development (DFID). Other governments have also taken the evaluation programmes seriously: the United States Millennium Challenge Corporation and the European Bank for Reconstruction and Development introduced planning of the evaluation and evidence for each programme proposal as one of the requirements.

- **Sharing knowledge in the network age: 'Scan globally, reinvent locally'**

It is generally recognised that new technology creates new opportunities for capacity building and allows the wider dispersion of development expertise. While it can be argued that circumstances in individual countries are rather unique and therefore their respective experiences cannot be directly replicated in other parts of the world, one also needs to recognise that knowledge can be gathered, analysed and adjusted to fit local needs. This assumption gave birth to a new motto: 'scan globally, reinvent locally'. The emergence of formal and informal networks around the globe allows for sharing ideas and knowledge beyond traditional North-South information flows. For instance, the Electronic Networking for Rural Asia Pacific project is supported by the International Development Research Centre (IDRC) and the International Fund for Agricultural Development..

Sources: GIZ (2012), OECD (2013), UNDP (2002)

Finally, in order to deal with the challenge of fragmentation at the global stage, it is imperative to address the question of a future architecture for capacity-building efforts. The currently prevailing multiplication of efforts leads to unnecessary duplications, hence providing overarching umbrella architecture for such activities could help streamline these efforts and improve efficiency in the use of limited resources. Such a framework could also help to clarify the roles of the United Nations agencies, regional organisations and other donors. Part of that effort should be also mainstreaming the role of cybersecurity elements in other policy areas essential for development and security, including in security sector reform efforts, law enforcement training courses, education and research programmes, etc.

Box 4: Building trust through aid transparency

The Busan Partnership agreement of 2011 reaffirmed the importance of aid transparency as one of the key requirements for improving the effectiveness of international development efforts and towards enhancing understanding and building trust across communities. In the absence of openness and transparency about where assistance goes and how the funding is spent, there is a risk that support for international involvement will decrease in donor countries (especially in light of current budgetary constraints) and those in the recipient countries will have doubts about the real intentions of the donors. Transparency is particularly important in the case of cybersecurity where the conceptual interlinkages between security, resilience and development are still only narrowly explored. Furthermore, the lack of transparency and oversight in domestic systems creates conditions for corruption and leads to inefficiencies. It would be therefore beneficial to expand the scope of the ongoing initiatives focusing on transparency and corruption in general. These include the following for instance:

- **Publish What You Fund** – a UK-based campaign group which assesses the transparency of more than 50 donor countries and international organisations. Their Aid Transparency Index monitors the availability and format of aid information (i.e. standardised information allows for better comparison between donors).
- **Transparency International** regularly publishes reports on the perception of corruption. In 2014 it has also published a report, 'Corruption as a Threat to Stability and Peace', that highlights the link between corruption and stability.

Sources: Publish What You Fund and Transparency International websites.

II. BUILDING BLOCKS FOR STRENGTHENING CYBERSECURITY CAPACITIES

Neil Robinson

The UN recognises that ICT connectivity is an increasingly important facet of social and economic development. In particular, the 2009 Report of the Millennium Development Goals Gap Task Force reflected on the persistence of the 'digital divide' between developed and developing countries and on the need to bridge this gap. However the world's growing dependence on the internet has revealed the vulnerability of cyberspace to disruption and attack, and highlighted the importance of a coordinated response at national, regional and global levels.

There is a range of instruments available at national level for addressing cyber threats and risks to critical infrastructures. Such measures take on different aspects depending on which part of a 'Prevent-Protect-Pursue-React' cycle they relate to. For example, measures to build capacity to prevent attacks and protect systems are long-term, diffuse and difficult to evaluate. Similarly, standards for enabling supply chain integrity require long-term strategic intervention whose benefits are difficult to gauge and which may not pay off for years to come. On the other hand, measures to detect attacks and react to them, being somewhat more tangible, often receive more attention from policymakers. Examples include capacity building for incident response teams. Consequently, managing risks includes a panoply of measures not just confined to technical solutions. Capacity building involves much more than simply installing anti-virus tools. It needs to cover a broad range of activities including training but also having the appropriate organisation, facilities and national-level policy (strategy, rules, processes, guidance) to deliver a useful capability. Many countries at present are doing this, either under their own initiative or spurred on by the policies of other international actors.

Given that security is often a poor cousin to functionality (especially for private sector owner operators) some responses taken by firms – in whose hands the majority of technical infrastructure is to be found – are clearly inadequate (e.g. under-investment in security). In addition to uncertainty posed by the problems themselves, other issues deserve consideration, namely: the complexity of the sheer number of stakeholders that need to be engaged; the challenges of being proactive in managing these risks; and the difficulty of understanding what overall purpose security measures should serve. Ultimately, like many areas of public policy, building national and regional capacity to tackle cybersecurity is a question of trade-offs and nuances.

In terms of specific actions, there would appear to be some common agreement coalescing around the need for a range of different elements to be in place. A number of studies and efforts undertaken so far across the globe allows for identification of the following four pillars: (i) concepts and strategies; (ii) laws and policies; (iii) organisation, and (iv) implementation.

Pillar one: concepts and strategies

When considering the development of national level capabilities to tackle risks in cyberspace a primary consideration is to determine what exactly it is that needs to be protected and how (see Box 1). This is the ultimate objective of any public policy intervention in this area. With the aforementioned spread of information technology (and the internet) many countries are extracting extensive economic and social gains from cyberspace. Most Western-oriented scholars appear to agree that protecting these economic gains is the key driver for cybersecurity efforts. Nonetheless, other initiatives point to different rationales for cybersecurity, involving protection of sovereignty or particular ethical or cultural values. Moreover, there are a number of countries which have not yet been able to properly identify what purposes cybersecurity should serve.

Pillar two: laws and policies

A clear legislative framework is often seen as an important (if not the most important) building block. This can cover a broad array of interconnected themes Relevant legislation often includes a panoply of laws and regulations. Three legal dimensions in particular have been central in recent debates:

- *Data protection and human rights* underline the need for the protection of personal data and the right to privacy of communications in the digital age. The principles encapsulated in the European Convention of Human Rights and the recent discussions on the right to privacy in the digital age in the United Nations provide some guidance in this respect.

- *Substantive criminal law* provisions usually aim to define types of misuse of computer and networked information systems. The Council of Europe Convention on Cybercrime of 2001 ('Budapest Convention'), for instance, provides three categorisations for this type of crime and offers a framework for international cooperation against cybercrime.

- *International legal framework* provisions that provide a framework for state behaviour on the international stage such as Article 51 of the UN Charter or international humanitarian law.

Box 1: Assessing the risks in cyberspace

It is possible to group risks in cyberspace into three main categories:

- *Cybercrimes*: cases in which computers are used to commit crime or are targeted for crime. Examples include theft of money or intellectual property, fraud, attacks on infrastructure or information systems.
- *Cyber espionage*: cases of intrusion into networks of other countries or companies whereby computers are used to extract large amounts of information for military, governmental or economic gains.
- *Cyber conflict*: cases where computers are used for military purposes, for instance to destabilise a country (e.g. Estonia), neutralise parts of the military installation (e.g. radars in Lebanon) or sites which could pose a threat (e.g. the Stuxnet attack on nuclear plants in Iran).

Assessing the exposure to each of these risks is a vital prerequisite for designing an appropriate risk mitigation strategy. Whereas the identification of the type of perpetrator (i.e. individual, organised group, state) does not play a big role in assessing the nature of the risk, it complicates designing appropriate responses. For instance, the classical law enforcement approach to cyberattacks committed by individuals is difficult to apply to state-sponsored groups. In May 2014, the US Department of Justice indicted five hackers from the Chinese People's Liberation Army for computer hacking, economic espionage and other offences directed at six American victims in the US nuclear power, metals and solar products industries. Most observers, however, agreed that this was a symbolic move since the chances that the Chinese would turn over the individuals named in the indictment are very low.

Outside of specific legislation, governments also turn to policy building blocks which can be articulated in strategic documents or more focused instruments. These might be national strategies to tackle cybersecurity; formal or informal declarative policy pronouncements or other types of non-binding official statements and 'soft law' (see Box 2). Their role, in addition to providing a comprehensive approach to cyber issues, is to send a signal to industry, the international community and potential adversaries about the weight attached to a specific issue. They are also significant by virtue of the process that leads to their development and adaptation, which by itself is an exercise in capacity building.

Pillar three: organisation

At the national level, some type of policy organisation with responsibility for overseeing cybersecurity is important. However, there are varying approaches to what shape and form it takes, driven by the nuances of national culture, history, law and

methods of public administration in the country (see Box 3). The main factor to bear in mind when appointing a body to take charge of cybersecurity at national level is that it needs to be capable of co-ordinating the implementation of a national cybersecurity strategy (NCSS). Such a body may be located in the ministries of justice, defence, telecommunications or a distinct central office supporting a national-level executive. A second type of increasingly common national organisation is a national-level Computer Emergency Response Team (CERT). A national-level CERT fits the role of last resort: an organisation theoretically able to coordinate and effect rapid responses and mitigation of national-level incidents. Implicitly, it can possess an overview of the country's cybersecurity status at a particular point in time. Apart from these two organisational constructs, other entities contribute to the level of cybersecurity capacity, including capabilities to perform national-level risk assessments, intelligence agencies, and regulators (i.e. data protection, telecommunications, consumer protection). For instance, law enforcement agencies often play a major role due to their interest in tackling cybercrime.

Latterly, defence ministries are being increasingly recognised as an important player but it is unclear whether this is driven by the evolving nature of cyber threats or a desire on the part of defence ministries to be seen as the security provider of last resort. Finally, it goes without saying that each ministry or government department is responsible for building its own cybersecurity capacity. Evidence from other countries suggests that the key criterion for selecting the most suitable organisation to take forward cybersecurity implementation might be the one with the broadest set of relationships with other stakeholders. Such an organisation must have (or be part of another entity that has) a voice and credibility to get a seat at the decision-making table, and especially have access to the Ministry of Finance when resource and budgetary considerations are at stake. Putting an organisation in a marginalised or low-ranking department in charge of cybersecurity implementation will mean that the establishment of capacity will be likely to fail.

Pillar four: implementation

Identifying the capacity-building pillars is just the beginning of the journey and the final outcome is very much dependent on how they are put in place. Ultimately, it is the implementation of the legal framework or a national cybersecurity strategy that determines the success or failure of the whole undertaking. Therefore, aside from these three vertical building blocks, there are a set of crosscutting horizontal factors that act as enablers for these elements.

Box 2: Designing a cybersecurity strategy

In 2012, the OECD published a report entitled *Cybersecurity policy making at a turning point: analysing a new generation of national cybersecurity strategies for the internet economy*. The report contained an overview of the latest generation of national cybersecurity strategies in ten countries who volunteered to participate in the study. The report highlights common themes in analysed documents, in particular their focus on enhancing governmental co-ordination at policy and operational levels in order to ensure economic and social prosperity by limiting the exposure to cyber threats. The authors also underline the evolution of almost all new cybersecurity strategies from protecting individuals and organisations as distinct actors to also protecting society as a whole.

Concepts shared by most strategies:

- Enhanced governmental co-ordination at policy and operational levels in order to ensure a clear division of labour within the government
- Reinforced public-private co-operation in recognition of the key role that the private sector and users play
- Improved international co-operation and the need for better alliances and partnerships with like-minded countries or allies, including facilitating capacity building
- Respect for fundamental values, including privacy, freedom of speech, and the free flow of information.

Emerging trends in cybersecurity strategies:

- Sovereignty considerations, in particular concerning intelligence and military aspects
- Flexible policy approach to reflect the evolving nature of the Internet
- The importance of the economic aspects of cybersecurity
- The benefits of a multistakeholder dialogue.

Following the adoption of a cybersecurity strategy, most countries develop specific action plans that aim at strengthening key priority areas, including government security, protection of critical information infrastructures, the fight against cybercrime, awareness raising, education, response and investment in R&D.

Source: OECD, 2012

Resources

Chief among these is investment to support achieving the objectives. In the current fiscal climate, with government debt at high levels and stagnating growth in many countries, the need for public investment in a topic as seemingly arcane as cybersecurity is a difficult argument to make. Nonetheless, some countries have taken these decisions – with additional investments for cybersecurity being headline news. For example, in 2010 the UK revealed it would spend £650 million (nearly €1 billion) on its cybersecurity programme, while in 2013 the French Defence Ministry

announced that it would be spending €1 billion on cybersecurity. Meanwhile earlier in 2014 President Obama set aside around $13 billion (€11billion) for cybersecurity in the US Federal budget request for 2015. These resources go primarily towards new centres or co-ordination functions, recruitment, law enforcement or facilities to support goals outlined in cybersecurity strategies. At the regional level too, budgets have been a characteristic of many cybersecurity capability building efforts. For instance, the European Cybercrime Centre (EC3) was funded to the tune of €8 million and NATO's NCRIC received €45 million funding. The involvement of the Ministry of Finance, as a key decision-maker, is in that respect essential for the successful activation of resources.

Box 3: Who manages cyber policy? Overview of different models

The organisational arrangements of individual countries place a strong emphasis on appointing a co-ordination point at the policy and operational levels. This role can be performed by a specific agency for cybersecurity attached to a co-ordination body (e.g. the French ANSSI), a Ministry (Canada, Germany, Netherlands) or in some cases to a cabinet office (e.g. Australia, Japan, United Kingdom) or a Head of State (e.g. the 'Cybersecurity Czar' reporting to the White House) in order to give it more political leverage.

- **Finland:** the Ministry of Finance's Government Information Security Management Board (VAHTI) for co-ordination with respect to cybersecurity within the government.
- **France:** a national authority for the security of information systems, the National Agency for the Security of Information Systems (ANSSI), attached to the Secretary General of Defence and National Security (SGDSN) who reports to the Prime Minister.
- **Germany:** the Federal Ministry of the Interior in cooperation with other ministries and in particular the Foreign Office and Ministries of Defence, Economics and Justice. A National Cyber Response Centre was created to optimise operational cooperation within the government.
- **Netherlands:** Ministry of Security and Justice and a National Cyber Security Centre responsible for strategic guidance and implementation. A National Cyber Security Council, on the other hand, brings together representatives from the public and private sectors as well as academia to help improve the understanding of cybersecurity developments.
- **United Kingdom:** Office of Cyber Security and Information Assurance (OCSIA) in the Cabinet Office. It provides strategic leadership for and coherence across the government. The 2009 Cyber Security Strategy also created a Cyber Security Operations Centre (CSOC) to actively monitor the health of cyberspace, provide collective situational awareness, enable better understanding of attacks against UK networks and users, and coordinate incident response.

Source: OECD, 2012

Skills and awareness

Training, education and awareness-raising are important factors in ensuring that cybersecurity mechanisms are robust and resilient (see Box 4). These educative capabilities are often based on the assumption that by ensuring that individuals (consumers; personnel) are better trained and more educated, the risks will decrease concomitantly. This is partly true. Any capacity-building efforts focusing on upskilling the human factor must recognise that there is a difference between training, education and awareness, and that there is a need to set objective frameworks or thresholds against which the effectiveness of those efforts could be measured. Anecdotal evidence from different countries suggests that those countries where cybersecurity implementation works well are those where there is a strong culture of IT governance norms.

Equipment and technology

Ironically, establishing the right technological building blocks for the virtual world requires a surprisingly high degree of physical infrastructure. The types of infrastructure include labs, cyber-ranges or test facilities, data centres etc. Technological security elements such as routers, servers and network devices are also required. Increasingly, these are provisioned and supported by the private sector that manages and runs such equipment on behalf of the government. However, such arrangements are by no means standard: in many countries the trend of outsourcing such services to a third-party private sector firm (Managed Security Service Provider) is non-existent or nascent.

Coordination

Implementing cybersecurity measures to mitigate various types of risks requires the involvement of a range of other types of organisations. It is commonly assumed that the private sector owns and operates the majority of infrastructure now deemed as 'critical' (although this has never been empirically determined) and therefore coordination with the private sector is a priority. Certainly, the regulatory tone set by many cybersecurity efforts in Europe, the United States and some countries in the Far East has, at least at face value, the character of being public-private. Another important coordinative endeavour is that conducted among peers on the international arena. A number of instruments that contribute to improve coordination include: information exchange (occurring in a private sector-driven group, usually among peers from a single sector); Public-Private Partnerships – a somewhat broadly defined mechanism for encouraging shared responsibility between the private and public sector; and Information Sharing and Analysis Centres (ISACs) – a private sector mechanism that functions as an information clearing house on a fee paying basis. Nonetheless, the question of information exchange between parties with such different agendas is by no means straightforward: evidence from analysing practices suggests that information exchange is bedevilled by complex issues concerning incentives and trust especially between organisations with competing motives such as the private sector and government, or law enforcement agencies and CERTs. On the international stage, global peer group

networks between governments, international organisations, and representatives of civil society and the private sector (i.e. the London Process, the Meridian Process, Commonwealth Telecommunications Organisation) also play a role.

Box 4: Building up cyber skills at schools: examples from the US

Multiple studies highlight the difficulty of meeting cybersecurity manpower needs. According to Gartner Inc. an estimated 300,000 cybersecurity jobs are vacant in the United States; among those, 60,000 could be filled by individuals who do not have a four-year college degree. At the same time, a study by RAND Corporation concluded that finding and retaining qualified individuals at what are considered reasonable wages is problematic in particular at the high end of the capability scale. In the United States, the efforts to develop a model outlining cybersecurity roles, responsibilities, skills and competencies are undertaken separately by the National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defence, Chief Information Officers Council, and US Office of Personnel Management (OPM).

Examples of government initiatives

NIST coordinates the National Initiative for Cybersecurity Education (NICE) aimed at improving cybersecurity education in the US, including efforts directed at the federal workforce. DHS and the National Science Foundation (NSF) run a Scholarship for Service programme which provides funding for cybersecurity education at both undergraduate and graduate level in exchange for a commitment by recipients to work for the federal government. A NSF grant was also provided for National CyberWatch Center K-12 (primary and secondary education) that holds an annual series of workshops for young girls to promote interest in cybersecurity careers. Based on the conviction that STEM education challenge is a national security issue, the National Youth Cyber Education Programme (CyberPatriot) was established in 2009. It is a competition to generate interest among high school students in science, technology, engineering and mathematics (STEM) education and encourage them to consider careers in cybersecurity.

Example of a private sector initiative

The Symantec Cyber Career Connection (SC3) was announced by Symantec at a meeting of the Clinton Global Initiative America in June 2014. The aim of the programme is to address the gap in the cybersecurity workforce and provide new career opportunities for young people. A pilot programme was scheduled to start in August in major US cities: New York, Baltimore and the San Francisco Bay Area. The pilot programme will include a cybersecurity curriculum developed by Symantec in partnership with non-profit making organisations, as well as a virtual mentorship programme designed to promote and familiarise students with the industry. Following their training, students will be placed in cybersecurity internships to learn about specific jobs: systems administrator network defence technician, etc. Symantec will help programme graduates seek jobs through its network of customers and partners.

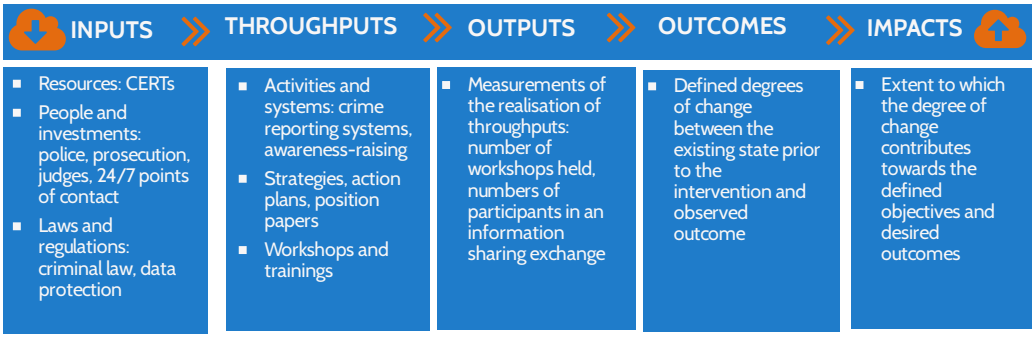
Sources: Libicki et al. 2014; Symantec and DHS websites.

From inputs to impact

Beyond all this, there remains the thorny question of understanding whether the measures identified above are having a demonstrable effect upon the intended outcome (which for Western Europe includes protecting economic growth and stimulating human development). The utility of models which attempt to map inputs, throughputs, outputs and outcomes to impacts is relevant here: although it might not be possible to fully map such a model, as is often the case in the cybersecurity domain the process itself is often more valuable than the end product.

Despite this, some important issues still need to be addressed. First and foremost is the need to be better at determining the threat, especially establishing the link between technical threat vectors and the nature and motivation of actors. Another key issue is the role of R&D support to rebalance the cycle between attack and defence. Investment in longer term research can offer solutions to some challenges, including technologies like stronger encryption or broader systematic agendas such as that of Next Generation Networks or Internet2. The need to consider R&D of course comes in the context of the ever-changing technology landscape – currently characterised by developments such as the Internet of Things, intelligent transport systems and convergence between embedded computing devices. A final issue worth exploring concerns evaluating effectiveness. Cybersecurity is a domain characterised by claims and counter-claims advanced by vested interests from all sides of the debate. Establishing what works and why has long been seen as the holy grail in this area. Therefore, when considering approaches to managing risks, it is important to adopt an evidence-based approach to assign due consideration to effectiveness and the relative benefits of any measure, compared with alternatives.

Figure 1. Capacity building in cyberspace: from inputs to impacts



In conclusion, when considering the implementation of capacity-building efforts, it is important to recognise that 'one size does not necessarily fit all'. Understanding the background context, structures and ways of working in a particular country, as well as strategic high-level priorities, is extremely important for identification and implementation of lessons from other practices. Care must be taken not to transplant policies, laws or lessons from one contextual setting to another, without first understanding the ways in which the contexts and characteristics are shared. Finally, capacity-building efforts need to be sensitive to local laws and practices and especially in a development context recognise that there may be very pressing competing priorities that sometimes take precedence over cybersecurity concerns.

III. RULE OF LAW AND HUMAN RIGHTS IN CYBERSPACE

Maria Grazia Porcedda

The internet and its World Wide Web have gradually become a platform facilitating economic, social and human development beyond the developed world. According to the United Nations' 2013 Human Development Report, internet connectivity is growing at a rapid rate throughout the world: 30% a year in 60 developing countries in the last decade. Such tremendous growth, often enabled by the parallel spread of mobile devices, contributes to empowering people across the globe by increasing their access to knowledge and services as well as supporting entrepreneurship and participation. To cite but one example, Digital Bangladesh – a national initiative to use Information and Communication Technologies (ICT) to implement and help meet goals in education, health, employment and poverty reduction – led to the creation of more than 4,000 Union Information Services Centres which provided access to government information, including examination results, birth and death registrations, and computer training.

Yet, challenges to making full use of the benefits offered by the internet persist, ranging from infrastructure-related shortcomings (e.g. limited or no access to fixed cables) to the evolving nature of cybercrime or growth of malware infections. At the same time, growing internet penetration also means that cybercrime is no longer a purely urban phenomenon. For instance, the 2013 data released by the Indian National Crime Records Bureau (NCRB) showed a jump of 122.5% in cyber offences in the course of 2012. Hacking accounted for almost 60% of all cyber offences in India, out of which 45% were reported from the 88 cities covered, and the remaining 55% originated in small towns or rural areas.

The risk that cybercrime undermines people's trust in cyberspace (e.g. by inflicting a financial loss), is significant and may ultimately stifle its great potential (see Figure 1). Therefore, for cyberspace to flourish, governmental institutions need to employ their resources in order to provide coordinated structures, shared norms, and the maintenance of security. The questions of whose security, and protection from what, are important ones. At the technological level, the security of cyberspace depends on the protection of network and information systems. But behind the technology there are people whose ultimate well-being depends to a large extent on a well-functioning institutional and legal environment. Consequently, the focus on an open and secure cyberspace addresses two important aspects of human security introduced in the Human Development Report 1994: freedom from want (i.e. by providing open and free access to the internet) and freedom from fear (i.e. by providing a secure environment for online activities).

It is therefore essential that pursuit of human security goes beyond the traditional focus on cybercrime and takes into account a broader vision of cybersecurity. Both can be successfully shaped through legal capacity building – i.e. the development, adoption and implementation of a legal toolbox (see Table 1). This effort is based on the premise that human rights and good governance (understood as the legal counterpart to human development), as well as cybersecurity, can be fostered by reshaping cyberspace in accordance with internationally endorsed principles of the rule of law.

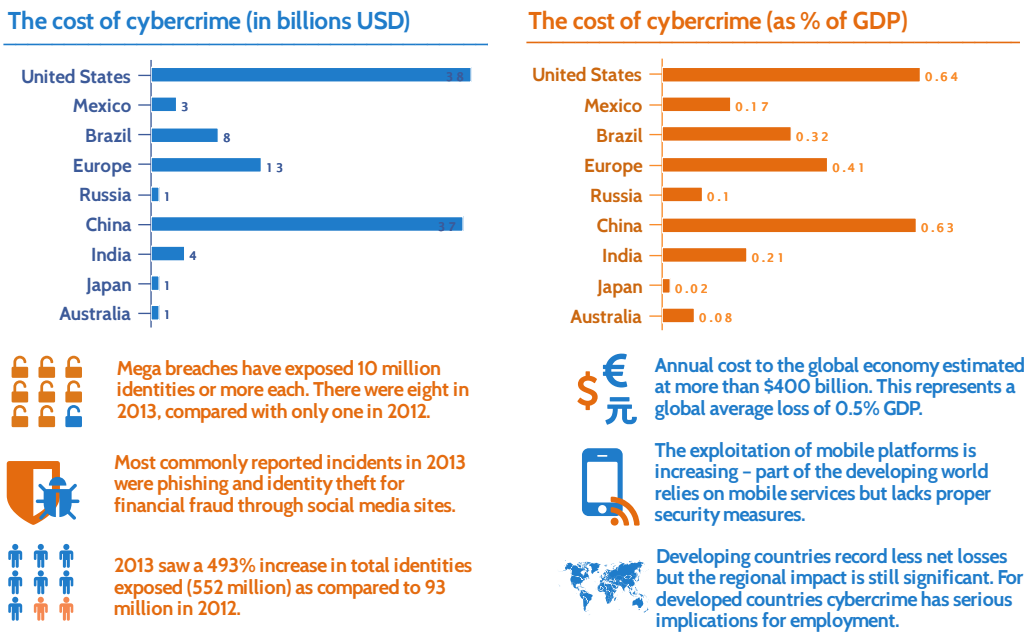
The challenges of legal capacity building beyond cybercrime

Cybercrime refers to crimes committed both against data and computer systems and by means of computer systems and it is only one of the key policy areas contributing to cybersecurity broadly defined. This complementarity has been reflected, *inter alia*, in the 2013 Cybersecurity Strategy of the European Union, which defined cybersecurity as efforts to preserve the 'availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein'. Cybersecurity hence has a broader connotation aimed not only at pursuit, but also prevention and protection, and ideally results in a more complete contribution to human security. If the goal of legal capacity building is to protect human rights and good governance (and ultimately promote human security and human development), then its focus should be more comprehensive, in line with this definition.

In practice, however, this approach has not been followed, not only because of the inherent complexity of tackling cybersecurity, but also because, being transnational, cybersecurity requires international cooperation. However, common legal capacity-building initiatives in cybersecurity are challenged by stark differences in legal systems, constitutional traditions and ideologies (e.g. concerning the scope of application of national laws with regard to internet governance, and the ultimate aims of an overarching cybersecurity strategy). While national cybersecurity strategies are being adopted ubiquitously (see Box 1), regional cybersecurity agreements, let alone an umbrella treaty under the aegis of the UN, are not on the horizon.

In contrast, common initiatives on cybercrime have proven easier, possibly because of the pre-existence of Mutual Legal Assistance schemes. Accordingly, legal capacity building has mostly focused on criminalisation and rules of procedure, including electronic evidence or investigative measures, both at the national and at the international level. Capacity building has come to mean enabling criminal justice authorities to meet the challenge of cybercrime and electronic evidence in both developing and developed countries. This entails strengthening knowledge and skills as well as improving the performance of criminal justice institutions, including their cooperation with other stakeholders in a sustainable manner.

Figure 1. Putting a price tag on cybercrime



Sources: Symantec Internet Security Threat Report, 2013; McAfee-CSIS Report on the Global Cost of Cybercrime, 2014

To be sure, there also exist differences in approaches and in the potential outcomes that different legal instruments can attain (see Boxes 1 and 2). The main achievement in this respect has been the adoption of the Budapest Convention (2001, ETS no. 185), the only binding international instrument addressing cybercrime that is open for accession by any country, independent of their geographical location. The Convention provides a framework for cooperation between countries and sets a general direction for national legislation against cybercrime. Despite its wide reach, the Convention cannot aspire to global ratification. The Fortaleza Declaration, adopted at the Sixth BRICS (Brazil, Russia, India, China and South Africa) Summit, clarifies that the countries will seek independent and common initiatives, as well as the elaboration of a common strategy at the international level.

Box 1: Legal capacity building: examples from Africa, Latin America and Asia

Tanzania is in the process of enacting three laws addressing cybercrime: the Computer Crimes and Cyber Crimes Bill, the Data Protection and Privacy Bill, and the Electronic Transactions and Communications Bill. All three are prepared in cooperation with the Bank of Tanzania. The existing challenges still include insufficient investigative capacity, lack of skills and the absence of a joint platform for legislature mechanisms, national enforcement and criminal justice.

Uganda passed laws related to the legal framework promoted by the East African Community in 2011: the Computer Misuse Act, the Electronic Transactions Act and the Electronic Signatures Act. The Computer Misuse Act is the primary legal document addressing cybercrime, including abuse or misuse of information systems. The limitations in investigative capacities were exposed in some high-profile cases like *Uganda vs. Kato Kajubi* and *Uganda vs. Aggrey Kiyingi*.

Panama approved the National Strategy for Cyber Security and Critical Infrastructure Protection (ENSC+IC) in early 2013. The ENSC+IC guides and coordinates all national efforts on cyberse curity. Its objectives include increasing the resilience of critical infrastructure to cyber incidents or attacks, cybersecurity education and awareness raising, strengthening partnerships and increased national and international collaboration. The National Authority for Government Innovation (AIG) – operating through the national cybersecurity incident response centre, CSIRT Panama – provides supervision and leadership regarding cybersecurity-related matters.

Colombia's efforts to fight cybercrime and improve cybersecurity are steered by the CONPES 3701 – a policy framework that defines guiding principles, delineates roles and responsibilities, and highlights priority areas for action. In addition, Law 1273 of 2009 provides a national legislative framework for cybersecurity and cybercrime. The specialised Police Cyber Center (CCP) operates within the National Police of Colombia.

Uruguay does not have a specific cybersecurity strategy but relevant guidelines have been embedded into related initiatives such as the government's Digital Agenda. The primary responsibility for the investigation of cybercrimes and related activities lies with the Computer Crime Unit of the National Police whereas the Agency for e-Government and an Information and Knowledge Society (AGESIC) – which also houses the national cybersecurity incident response centre – is the lead authority for general cybersecurity issues.

Sri-Lanka developed its cybersecurity legislation in 2003 using the Budapest Convention as a model law. Its capacity-building programme, based on an integrated development agenda and a partnership with the World Bank, resulted in a very successful CERT selected in 2013 for the cybersecurity drill of the Asia-Pacific area.

Sources: Reports from regional workshops organised by ECOWAS and OAS.

A potential response: the rule of law

The challenge for legal capacity-building in cyberspace lies in sidestepping normative differences so as to build mutual trust and eventually foster international initiatives. Working on objectives capable of rallying consensus is certainly a step in this direction. However, the international community already possesses a promising common framework. The United Nations (S/2004/616) and its member states, including BRICS, as well as other regional organisations (see Council of Europe, CM 2008/170), have progressively recognised the principles of the rule of law as a crucial element in shaping the relations between public institutions and improving mutual trust in the functioning of the judiciary and criminal justice institutions.

In order to foster human rights and human security in cyberspace, the tenets of the rule of law need to be adapted to cyberspace and embedded in legal capacity building. Taking inspiration from the 2011 report of the Venice Commission, the rule of law calls for:

- *Legality*: actions in cyberspace must be based on laws that regulate the conduct of public and private actors (including liability of companies), protect (cyber)security, sanction (cyber)criminal activity and de-criminalise lawful and constructive behaviour, e.g. through ensuring a stringent legal framework for undercover investigations of cybercrime cases, including the role of 'white hat hackers'.

- *Legal certainty*: applicable laws governing cyberspace must be unambiguous (e.g. address overlaps between civil and criminal law), easily accessible (public campaigns), and properly implemented and enforced.

- *Prohibition of arbitrariness of the executive powers*: measures (rules or tools) applying to cyberspace must include safeguards, such as strict permissible limitations. Public and private bodies enforcing security must adhere to principles of fairness, reasonableness and accountability. This is particularly important in cases where cooperation between several agencies is required.

- *Access to justice*: the applicability of law must be clear; standards for the collection and admissibility of evidence must be defined. Concrete actions in this context include developing and using forensics to solve the problem of attribution. In that context, it is also important to ensure that convicted cybercriminals are not only appropriately and proportionately punished, but that policies are developed for their incarceration and reintegration.

- *Non-discrimination and equality before the law*: laws governing cyberspace must apply to all in an equal and uniform manner.

- *Respect for human rights*: Respect for human rights is both a component of the rule of law and an independent objective to which all members of the United Nations subscribe.

> Laws governing cyberspace must address states' positive and negative obligations to respect, protect and fulfil human rights. This includes conforming to internationally recognised standards on human rights, as well as addressing the potential impact on rights of laws applying to cyberspace.

While these tenets are adapted from a regional organisation, the principles they express are recognised worldwide. The application of principles of the rule of law to cyberspace entails providing for the professional development of interlinked and properly communicating bodies, such as CERTs who block attacks and study solutions, special police units, prosecutors and judges who handle cybercrime cases, and data protection authorities. This requires a long-term commitment, including putting in place adequate infrastructure, remuneration and training.

Human rights

As highlighted above, legal capacity building in cyberspace requires an integrated approach to human rights (see Table 1). To achieve this, it is important to overcome three trends derived from the prevalent focus on cybercrime in capacity building.

First, the focus on rules of procedures and forensics might lead to a lowering of the standards of protection of rights. For instance, article 14 of the Budapest Convention on Cybercrime allows the same often-sweeping procedural rules to be applied to the collection of electronic evidence for any type of criminal investigation online. According to legal scholarship, clauses on human rights (e.g. article 15 of the Budapest Convention on Cybercrime), must be specified and developed nationally. It is for states to attach strict safeguards to investigative powers by clarifying the permissible limitations to rights (e.g. legal basis, satisfaction of a legitimate aim, proportionality etc.), but this might not be the reality in all states implementing the Budapest Convention.

Second, the approach whereby rights are taken into account only in relation to investigative measures negatively affects states' obligations. In fact, the rights requiring protection are not only those of the victims and perpetrators of cybercrime (the latter in the context of criminal investigations), but include those of citizens online (see Box 3). The 2001 Human Development Report clearly acknowledged the need to focus on the full catalogue of human rights in cyberspace by highlighting their importance for human development, and vice versa. Examples of promising steps in this direction include the recently adopted Council of Europe's Guide to Human Rights for Internet Users (2014) and the EU Human Rights Guidelines on Freedom of Expression Online and Offline (2014). Both documents refer to the duty of the state to respect, protect and fulfil/promote rights online as they do offline: rights to privacy (the right to respect for private and family life and the right to the protection of personal data), freedom of expression, freedom of information, freedom of association, freedom of religion etc. The documents recognise the importance of evidence collection, and therefore the need to limit the scope of application of those rights, but only to the extent permissible by a strict enactment of the rule of law tenets.

Third, the focus on cybercrime, rather than cybersecurity, overlooks the importance of prevention and existing synergies between the pursuit of cybersecurity and the protection of rights, such as those to privacy. Examples include preventive strategies such as protecting the confidentiality and integrity of communications, securing data and punishing those responsible for data breaches (see Table 1). The strategies required for prosecuting cybercrime can undermine the preventive strategies required for cybersecurity and the protection of the rights to privacy, thereby leading to a dilemma that must be eventually addressed.

Box 2: Legal capacity building at the regional level

On 27 June 2014 Heads of State and Government of the African Union (AU) approved the **African Union** Convention on Cyber Security and Personal Data Protection. This terminates the process launched in 2011 by the UN Economic Commission for Africa (UNECA) and the African Union Commission (AUC). The aim of the Convention is to harmonise African cyber legislation on e-transactions, cybersecurity, personal data protection and combating cybercrime. It seeks to define broader orientations for cybercrime repression strategies in member states of the AU and seeks to modernise cybercrime repression instruments by formulating a policy for the adoption of new incriminations specific to ICT. The Convention reaffirms the importance of protecting the rights of citizens in adopting legal measures in the area of cybersecurity, in particular those guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others.

Already in 2005, the **East African Community** (EAC) acknowledged that a legal framework on cybersecurity was a prerequisite to increase regional trade and investment, for the implementation of e-government initiatives and for harmonising laws and migrating towards a common market with a shared currency. Since then, EAC countries have hosted workshops to identify cyber laws, e-justice and information security as key cross-cutting issues that need to be addressed for a successful implementation of e-government and e-commerce in East Africa. The **Economic Community of West African States** (ECOWAS) has adopted legal instruments on cybercrime and personal data protection. The Directive on Fighting Cybercrime (2009) provides a legal framework for the member states, which includes substantive criminal law dealing with offences specifically related to ICT. Similarly, in February 2010 the ECOWAS adopted the Supplementary Act on Personal Data Protection, which establishes a framework for the collection, processing, transmission, storage and use of personal data to be implemented by ECOWAS members. The **Southern African Development Community** (SADC) adopted the SADC Model Law on Computer Crime and Cybercrime in November 2012. The process was initiated in 2005 when member states decided to harmonise legislation to combat cybercrime and improve cooperation between them on issues pertaining to extradition and electronic evidence.

Box 2 (continued)

A framework to fight cybercrime was introduced in the **ASEAN** Plan of Action to Combat Transnational Crime and supplemented by the work programme adopted in 2002. The cybercrime component encompasses five main areas of cooperation: information exchange, legal matters, law enforcement matters, training and capacity building, and extra-regional cooperation. The follow-up included the adoption of a common framework for ASEAN cybercrime enforcement capacity building in support of the global fight against cybercrime (2007) and the establishment of a Working Group on Cybercrime (2013). The discussions about cybercrime cooperation unfolded simultaneously in the **ASEAN Regional Forum** (ARF), which in 2006 adopted the Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space (US and Russia were not members at that time). The key elements of that statement include the acknowledgement of the importance of developing national frameworks for cooperation in addressing the criminal use of cyberspace and a call to enact and implement cybercrime and cybersecurity laws in particular concerning the prevention, detection, reduction and mitigation of attacks. The ARF members have also agreed to work together to improve their capabilities to adequately address cybercrime, including the terrorist misuse of cyberspace, through enhancing confidence among different national Computer Security Incident Response Teams (CSIRTs).

The **Organisation of American States** has taken the lead in strengthening cybercrime cooperation across the Americas. In 2004, the OAS Member States approved 'The Inter-American Comprehensive Strategy to Combat Threats to Cyber Security' which outlined a multidimensional and multidisciplinary approach with clearly defined mandates for the Inter-American Committee against Terrorism (CICTE), the Inter-American Telecommunications Commission (CITEL), and the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA) and its Group of Governmental Experts on Cyber-crime. CICTE and the Cyber Security Programme are committed to developing and furthering the cybersecurity agenda in the Americas, including strengthening cybersecurity capacity in the member states through technical assistance and training, crisis management exercises, and the exchange of best practices. REMJA, on the other hand, focuses on policy and technical debates related to the strengthening of and access to justice and international legal cooperation in areas related to mutual legal assistance in criminal matters, cybercrime and forensic sciences, among others. In 2012, the members of OAS adopted a Declaration on Strengthening Cybersecurity in the Americas which reaffirmed the importance of enhancing the security and resilience of critical information and communications technology infrastructure against cyber threats.

Sources: Reports and websites of regional organisations; EUISS exchanges and interviews with officials.

Good governance and accountability

Good governance, understood as law-making based on the participation of all potential recipients and openness, should complement respect for human rights in legal capacity building. This also entails accountability as a mechanism to ensure a virtuous process of policy assessment and improvement among all stakeholders. The role of civil society organisations in promoting human rights and good governance is broadly acknowledged, primarily due to the contribution they make towards empowering the rights-holders, fostering accountability and transparency, and raising awareness. A subject that still receives less attention, however, is the role played in this sense by the private sector.

Even though ICT companies and operators have to comply with local legal frameworks, their specific policies may have significant implications upon people's access to information or freedom of expression and, ultimately, participation. This fact has been acknowledged in the UN 2011 Guiding Principles on Business and Human Rights, which calls on business representatives to consider the human rights impact of their policies and to minimise their negative impact if needed – a move which may entail a loss of revenue for many companies. An example is the ban imposed by some governments on the sale of deep packet inspection engines to dictatorships during the Arab Spring.

A classic tool in cybersecurity and the fight against cybercrime is the establishment of public-private partnerships (PPPs) at the national, regional, and international levels. The PPPs can be the 'soft' key to the achievement of good governance-oriented cybersecurity, if some of their shortcomings are addressed (i.e. their fragmentation and their development outside of clear and binding legal frameworks). Comprehensive cooperation focuses mostly on traditional crimes committed by means of computer systems, whereas cybersecurity-related matters tend to be discussed in closer circles, thus limiting accountability. Moreover, PPPs are often based on the informal participation of private actors in what has been called 'tilting': the private actor shifts between the state and the citizen-user, breaking their relationship of trust (and law). Tilting in the governance of security challenges the application of the tenets of the rule of law, because it sidesteps the 'emergency brakes' that safeguard against abuses and violations of human rights. By relying on private actors, security is pursued in a legal vacuum that diminishes the involvement and protection of interested parties and challenges judicial review. In the absence of a clear legal framework, the other tenets of the rule of law crumble. A corollary is that human rights cannot be sidestepped, nor citizens' participation be limited, by means of informal arrangements, as only the law can establish the grounds for permissible limitations and offer effective remedies. In other words, good governance cannot exist without respecting the rule of law (see Table 1).

Box 3: Protecting human rights in cyberspace as a means of enhancing development

In recognition of the growing role of new technologies in providing access to information, stimulating participation, increasing accountability and as a means to express views, the European Union adopted the Human Rights Guidelines on Freedom of Expression Online and Offline in May 2014. The Guidelines state that all human rights that exist offline must be protected online, in particular the right to freedom of opinion and expression and the right to privacy. The purpose of the document is to offer to EU officials a practical set of guidelines on how to identify possible breaches of human rights and how to proceed in such cases. A number of issues pose a peculiar policy challenge, including attempts to block, jam, filter, censor or close down communication networks or protection of privacy. For instance, some reports suggest that following the military *coup* in Thailand in May, the junta established new administrative bodies to monitor and control online content and expanded surveillance of mobile messaging applications and social media activities which resulted in the arrests of activists and former government officials.

The EU's approach was further strengthened with the adoption of a human rights-based approach (HRBA) to development cooperation, encompassing all human rights. The EU recognises that 'the promotion of human rights, democracy, the rule of law and good governance and of inclusive and sustainable growth are the two basic and mutually reinforcing pillars of the EU's development policy'. Consequently, HRBA changes the analytical approach and integrates human rights into the design, implementation, monitoring and evaluation of all development policies and programmes. That is of particular importance in the case of legal capacity building given that the EU provides funding for cyber capacity-building projects implemented by the Council of Europe and increasingly engages in independent implementation of cybersecurity projects. Following the HRBA approach in legal capacity building would imply, for instance, ensuring that law enforcement and justice reform programmes take into account the rights component (see Table 1 for specific examples).

Sources: Council of the European Union (2014), European Commission (2014).

Conclusion: Avoiding 'cyberwashing'

Legal capacity building in cyberspace does not come without challenges. It depends on continued political support and getting the incentives for economic and social actors right: for the former, these include a fiscal regime rewarding best practice, but also the prospect of liability, and for the latter, usability, cost-effectiveness of education and the existence of alternatives. Furthermore, it affects the diverse activities taking place in cyberspace and the conflicting social and legal norms such activities build on. Finally, given the transnational nature of cybersecurity and the fight against cybercrime, it requires regional and international/inter-regional cooperation. The adoption of national cybersecurity strategies and policies is a necessary but insufficient step. Current regional initiatives are hampered by fragmented and sometimes clashing

legal frameworks, not least because of the differences in norms underpinning them. Yet, existing actions seem to share common languages (the importance of ICT for development) and objectives (e.g. developing criminal and procedural law, police and judicial training, and education) (see Box 2).

But the greatest challenge of a cybersecurity policy geared to human development is to avoid cosmetic changes or 'cyberwashing'. Formal adherence to the rule of law, good governance and respect for human rights in capacity building cannot be a substitute for implementing reforms and following them up. On the one hand, legal capacity building should take place in the framework of a continued partnership between the private sector, international organisations and development agencies, and hinge on its power to achieve the right combination of stimuli to support a human development-oriented global fight against cyber insecurity. Stimuli include the careful use of positive incentives (investment, membership in organisations, access to international networks) and negative sanctions (naming and shaming, freezing investment), in connection in particular with rule of law-compliant capacity building.

On the other hand, legal capacity building should be based on the prior identification of areas that require regulation. Dividing the cyber domain into five building blocks – the networks, the internet architecture (the logical highway), the data, terminal equipment, and users – could provide a useful framework for advancing human rights and rule of law agenda in cyberspace (see Table 1).

Law-making in each block ought to be based on a careful analysis of the structure of incentives, the potential security issues (the nature of the threat and the response required), the likely clashes and synergies in legislation across blocks (criminal vs. civil law, preventive vs. reactive measures), and the rights that can be affected by actions taken at each step. In fact, the rights implicated are not only those connected to defendants and plaintiffs in criminal investigations and disputes, but also the rights of citizens using the internet (freedom of speech, of association, data protection etc.) or performing activities that depend on the internet's infrastructure. Protection of citizens' rights in this domain cannot be underestimated if the legal capacity building is to enhance security and contribute to human development. Finally, law-making in each block ought to be supported by consultations with recipients, according to the most common and workable practices of participation in each country.

Table 1. Blocks of legal capacity building

1. The networks	Physical networks made of 'dumb' communication channels (physical cables, radio waves etc. functioning according to the end-to-end principle) and routers.	
	1a. Threats	Breakdown caused by human action (Stuxnet, Flame) or nature (tsunami)
	1b. Consequences	Disruption of the functioning of crucial services of society connected to the network.
	1c. Affected rights	**Rights of people at large:** right to life and to health, environmental protection. **Rights of defendants:** right to liberty and security; presumption of innocence and right of defence; principles of legality (*nullum crimen sine lege*) and proportionality of criminal offences and penalties; right not to be tried or punished twice in criminal proceedings for the same criminal offence (*ne bis in idem*).
	1d. Legal action needed	**Enacting laws:** • Protecting the physical networks as critical information infrastructure (CII); • Laying out security obligations for owners of infrastructure; • Establishing criminal provisions and setting appropriate sanctions. **Planning recovery and resilience after disasters**
2. The internet architecture	The logical highway made up of protocol stacks and layering that regulate the flow of data packets: • Physical: transmits units of information across the communication channels; • Link: presents the raw transmission as a dedicated, flawless connection; • Network: takes care of the communication between sender/recipient through routing; • Transport: divides the message into packets and numbers them; • Content layer: provides protocols for the front-end services, e.g. HTTP for the Web.	
	2a. Threats	Challenges to the security canons of stored or transmitted data or the related services offered by or accessible via that network and information system: confidentiality, integrity, availability (CIA).

	2b. Consequences	Laying the basis for many crimes against the data (art. 2-8 Budapest Convention); Illegal interception (breach of confidentiality) and System interference (DoS/DDoS, spam if criminalised) (art. 3 and 5 Budapest Convention).
	2c. Affected rights	**Rights of the users:** Data protection; privacy; right to property; consumer protection; right to an effective remedy and fair trial. **Rights of defendants:** right to liberty and security; presumption of innocence and right of defence; principles of legality (*nullum crimen sine lege*) and proportionality of criminal offences and penalties; right not to be tried or punished twice in criminal proceedings for the same criminal offence (*ne bis in idem*).
	2d. Legal action needed	**Enacting laws:** • Network and information security; • Data protection; • Laying out security obligations for internet service providers; • Liability (for ISPs and users); • E-commerce; • New criminal offences; • Investigative methods and procedures; • International rules on evidence sharing and applicable law. **Establishment of CERTs and regulatory bodies, and technical advisory bodies** **Police and judicial training on forensics and the problem of attribution** **Training judicial authorities and police**
3. Data transported	Transported by packets in accordance with the principle of net neutrality (delivery follows best effort regardless of the content carried). Content, traffic and location data can (in)directly identify individuals (personal data).	
	3a. Threats	Danger for security canons (CIA), but also authenticity and non-repudiation.
	3b. Consequences	Illegal access (hacking), illegal interception, data interference (spam), (art. 2-5 and 6 Budapest Convention); Computer-related forgery and Computer-related fraud (art. 7 and 8 Budapest Convention).

	3c. Affected rights	**Rights of the users/victims:** same as 2c. Possible spill-over effects on other rights: freedom of thought, conscience and religion; freedom of expression and information, freedom of assembly and of association; the rights of the child. **Rights of defendants:** same as 2c.
	3d. Legal action needed	**Enacting laws:** • same as 2d; and in addition • Security obligations for software providers; • Liability (for software providers and users); • Data retention; • Investigative techniques and safeguards. **Training judicial authorities and police** **Computer literacy for all**
4. Terminal equipment	'Clever' machines or terminal equipment connected by dumb channels, e.g. routers, PCs, mobile devices (smartphones/ tablets), sensors, RFID-enabled objects.	
	4a. Threats	Machines as the targets of and instruments used to perpetrate attacks
	4b. Consequences	Computer zombies, botnets, etc.
	4c. Affected rights	**Rights of the users/ victims:** same as 3c. Possible spill-over effects on freedom of thought, conscience and religion; freedom of expression and information, freedom of assembly and of association, the rights of the child. **Rights of the defendants:** same as 3c.
	4d. Legal action needed	**Enacting laws:** • same as 3d; • Laying out security obligations for hardware providers; **Training judicial authorities and police** **Computer literacy for all**
5. Users	People who ultimately control the devices and are behind communications, security and perpetration of crimes. People who leave an electronic trace of their offline conduct.	

	4b. Consequences	Misuse of devices (art. 6 Budapest Convention) and offences related to child pornography; offences related to infringement of copyright and related rights (art. 9 and 10); acts of a racist and xenophobic nature (Additional protocol); Use of the internet for recruitment of terrorists.
	4c. Affected rights	**Rights of the users:** same as 4c, plus freedom of thought, conscience and religion; freedom of expression and information, freedom of assembly and of association; the rights of the child. **Rights of defendants:** same as 4c.
	4d. Legal action needed	**Enacting laws:** • New forms of criminal conduct; • Investigative procedures for evidence of crime other than cybercrimes. **Planning appropriate information campaigns and training of users**

IV. ACHIEVING GROWTH THROUGH CYBER RESILIENCE[1]

Elena Kvochko

Pervasive digitisation, open and interconnected technology environments, and sophisticated attackers, among other drivers, mean that the risk from major cyber events could significantly slow the pace of technological innovation over the coming decade. Many leaders in business, civil society and government realise that for the world's economy to fully derive the value inherent in technological innovation, a robust, coordinated system of global cyber resilience is essential to effectively mitigate the risks of cyberattacks. This view is beginning to permeate discussions among senior leaders in the private and public sectors, and across different industries, as concerns related to cyber resilience shift from awareness to action. Addressing the problem will require collaboration across all participants in the cyber resilience ecosystem. But many questions remain on direction and responsibilities. In contrast, a much clearer picture is emerging of the actions that institutions should take to protect themselves. They should act now to enhance capabilities while a broader model for resiliency develops. Finally, given the strategic decisions required, chief executive officers, government ministers and other key stakeholders from civil society must engage directly with one another to put the right policies and plans in place.

Key trends

Research conducted by the World Economic Forum (WEF) in 2013-2014 assessed, *inter alia*, the key action areas for building global cyber resilience, and examined the impact of cyberattacks and response readiness. The results, presented in the report *Risk and Responsibility in a Hyperconnected World*, have pointed to two important aspects.

First, cyber threats and the risks of cyberattacks are starting to have an impact on business. Controls put in place to protect information assets have at least a 'moderate' impact on front-line employee productivity for nearly 90% of institutions. Moreover, security concerns are already making companies delay implementation of cloud and mobile technology capabilities. And while direct cyber resilience spend represents only a small share of total enterprise technology expenditure, some Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) estimate that indirect or unaccounted security requirements drive as much as 20-30% of overall technology spending.

1 The chapter is adapted from a contribution to a wider research project by the World Economic Forum (WEF) entitled *Risk and Responsibility in a Hyperconnected World*.

Second, current trends could result in a backlash against digitisation, with a huge economic impact. Major technology trends like massive analytics, cloud computing and big data could create between US$9.6 trillion and US$21.6 trillion in value for the global economy. If attacker sophistication outpaces defender capabilities – resulting in more destructive attacks – a wave of new regulations and corporate policies could slow innovation, with an aggregate economic impact of around US$3 trillion.

Against this background, the study found that large institutions lack the information and processes to make and implement effective decisions about cyber resilience. Overall, a large majority of firms have only nascent or developing cyber risk management capabilities. Most large institutions do not systematically understand which information assets need to be protected, who their attackers are, what their risk appetite is or which is the most effective set of defence mechanisms. Companies that spend more on cyber resilience do not necessarily manage cyber resilience risks in a more mature way – many are simply throwing money at the problem. In addition, almost all CIOs and CISOs say they cannot 'do it alone'. They believe a broader cyber resilience ecosystem must be put in place that spans not only the enterprise users of technology, but also technology providers, regulators, law-enforcement and other related institutions. However, views vary widely on the responsibilities and effectiveness of several possible public sector initiatives.

The in-depth analysis of the situation in the private sector helped to formulate three alternative scenarios in which economic value from technological innovations is realised or lost depending on models of cyber resilience. The study drew on knowledge and opinions derived from a series of interviews, workshops and dialogues with global executives and thought leaders to estimate the potential value to be created by technological innovations in the years leading up to 2020. It examined the value that could be put at risk if the adoption of such innovations is delayed because more frequent, intense cyberattacks are not met with more robust cyber resilience.

Scenarios for cyber resilience

The private sector agrees that a rapid expansion of technology innovations will significantly influence the way people think and interact with each other (see Box 1). E-commerce, mobile internet or social technologies are already used across the world: the social network Facebook has about 1,280 million users and represents a market value of US$183 billion; the Hangzhou-based Alibaba Group provides a number of internet-based services. According to *The Economist*, it is currently the second biggest internet company with the peak market valuation amounting to US$200 billion.

At the same time, cloud computing, the Internet of Things, autonomous and near-autonomous vehicles, and next-generation genomics are progressively reshaping our societies. It is estimated that these innovations could generate between US$9.6 trillion

and US$21.6 trillion in economic value between now and the end of this decade. But unless a secure, robust cyber resilience environment spanning the public and private sectors is created this prediction might never materialise. As a matter of fact, the World Economic Forum study argues that if rapidly increasing cyberattacks are met with less rapidly increasing protection capabilities, a backlash against digitisation could leave as much as US$3.06 trillion of that value unrealised.

Taking into account these two elements – the pace of increase in the intensity of the cyber threat and the pace of increase in the quality of response from private institutions and the public sector – it is possible to construct the following three scenarios:

- *Muddling into the future*: In this baseline scenario, attackers retain an advantage over defenders who continue to respond to threats reactively, albeit successfully. The level of threat increases incrementally, and more sophisticated attack tools consistently leave defenders trailing behind attackers. The adoption of innovative technologies slows, and as much as US$1.02 trillion in value generated from technological innovation is left unrealised over the next five to seven years.
- *Backlash decelerates digitisation*: In this scenario, the frequency of attacks significantly escalates, and international cooperation to combat the proliferation of attack tools proves elusive. Government cyber resilience regulations become more directive, disrupting the adoption of innovative technologies. As much as US$3 trillion in potential value creation from these technologies remains unrealised.
- *Cyber resilience accelerates digitisation*: In this scenario, proactive action from the public and private sectors limits the proliferation of attack tools, builds institutional capabilities and stimulates innovation. A vital cyber resilience ecosystem serves to facilitate and connect company operations. Technological innovation is enabled, accelerating digitisation and creating between US$9.6 trillion and US$21.6 trillion in value over the remainder of this decade.

It is estimated that in the coming years the annual spending on cyber resilience is likely to rise, from US$69 billion in 2013 to US$123 billion annually in 2020. But the extent of the increase and the return on investment will vary. Considerable disagreement exists among private sector actors about how to reach a consensus that could benefit all. Relationships between private and public institutions are unformed in many cases. Consensus is limited across industries, as well as across the private and public sectors. Insurance executives indicate that individual companies and institutions may have the strongest impact in fending off cyber risks. On the other hand, the high-tech sector and the largest corporations – those with a market cap of more than US$50 billion – indicate that technology vendors may be in a position to have the strongest impact.

Box 1. Big data commons: Data for Development (D4D)

Data commons is a term introduced to highlight the fact that data is more valuable when shared because it can inform decisions regarding government, public health or transportation systems. The massive volumes of data produced automatically by computers without human intervention – commonly referred to as big data – gave birth to a new term 'Digital data commons'. These are generated as side effects of our daily life: digital transaction records, mobile phone location fixes, road toll records, digital images, videos posted online, just to name a few.

Data for Development (D4D) is a concept born of the idea that big data could be used to improve the lives of people around the world. For instance, research groups from Serbia, Switzerland and the UK have demonstrated that by making some small changes in the public health system it might be possible to cut the spread of flu by 20% as well as significantly reduce the spread of HIV and malaria. Researchers at University College London, on the other hand, developed a method for mapping poverty from the diversity of mobile phone usage. Their project was based on the assumption that as the amount of disposable income increases, people explore their environment more, thereby diversifying their patterns of phone calls. The estimate of their disposable income was measured by assessing this additional exploration.

Another project was implemented in Côte d'Ivoire where about 90 research organisations from around the world provided their analysis of data describing the mobility and call patterns of the citizens, which can help in taking decisions about investment programmes for transport infrastructure. Building on the outcome of this project, Sonatel and the Orange Group have launched 'Data for Development Senegal' with the objective of contributing to the development and welfare of the population. The project focuses on five priority subjects defined in collaboration with responsible Ministries or the partner institutions: health, agriculture, transport/urban planning, energy and national statistics.

Sources: World Economic Forum, *The Global Information Technology Report 2014*; D4D and Orange websites.

Putting the house in order

Traditional approaches to cybersecurity appear increasingly ineffective. In most cases, businesses rely mainly on passive measures, typically addressing issues only after they have arisen. Business partners are not sufficiently involved, and the policing and application of cyber resilience lack consistent rigour. Responses are often backward-looking, require specialised talent that is costly and hard to find, and rely mostly on technology solutions, even though sophisticated agents often attack the weakest link: customers and employees.

There is a near universal agreement among Chief Information Security Officers (CISOs) and Chief Technology Officers (CTOs) that a step-change improvement

is needed in their own capabilities to protect their businesses from increasingly sophisticated cyber threats, enable productivity and innovation, and maintain a competitive cost position. Equally worrisome, a large majority of participants in the Forum interviews and workshops believe that attackers will continue to increase their lead over defenders. The prevailing view is that the sophistication or pace of attackers will increase more swiftly than the ability of institutions to defend themselves. Of particular concern is the dissemination of sophisticated hacking and attack programmes. To date, state entities have managed to control attack programmes aimed at disrupting their victims' operations and activities. But executives worry that such programmes will make their way to a wider variety of attackers with more destructive intent.

A survey conducted by the World Economic Forum points to gaps across sectors in current risk management capabilities. Of the 100 companies whose cyber risk management processes were examined, 90% had 'nascent' or 'developing' risk management capabilities. Only 21% were rated 'mature' or better on four or more of the eight practice areas studied. Institutions can be segmented based on the sophistication of their risk management capabilities and the scale of their cyber resilience expenditure. Spending and enterprise maturity are not correlated, however. 'Unprotected' companies spend little and spend it poorly. Others punch above their weight by spending little but doing a better job of risk management. Still others, the 'well-protected', spend vigorously and have relatively good capabilities for extracting value from their investment. Finally, some seem to throw resources at the problem, spending a great deal of money without much risk management sophistication.

The research also showed that banking is slightly more mature than other sectors in terms of cyber resilience capabilities. The largest companies across sectors are also slightly more mature than smaller ones. Variations within a sector and a size band are much larger than variations between sectors and between size bands. Even the largest firms have substantial room for improvement. For example, while financial services organisations tend to be more mature than other sectors, senior non-technical executives still struggle to incorporate cyber risk management into enterprise risk management discussions, and often are unable to make informed decisions because of lack of data.

Speed, mobility and collaboration are the hallmarks of the successful company in the digital age. But as cyberattacks proliferate, executives have to devote more attention to protecting vulnerable operations, often by imposing controls that create friction in critical functions. So far, cyberattacks appear to have had only a limited impact on research and development (R&D) plans, except in high-tech firms. Only about 25% of surveyed executives in the banking and healthcare sectors, and 17% in insurance, say that they would have to change the nature of their R&D investments to retain their value in the face of cyberattacks even if their underlying intellectual property is stolen. In the high-tech sector, fully half say they would have to change the nature

of their R&D efforts over time. Concern is apparent, however, about cyberattacks weakening value capture from cloud computing, mobile technologies and some healthcare technologies. About 78% of companies surveyed say security concerns delayed the adoption of public cloud computing by a year or more, and 43% note that such concerns delayed enterprise mobility capabilities by the same length of time.

Cyber resilience controls are having a significant impact on front-line productivity. About half of companies overall said that controls had at least a moderate impact on end-use productivity. Half of the high-tech executives cited existing controls as 'a major pain point' for users and as limiting the ability of employees to collaborate. Actual spending on cyber resilience may also be much higher than most executives assume, the research indicates. 'Indirect' spending on information technology (IT) security to adjust to new risks and provide ongoing responses to cyber risks may be a significant cost driver for IT organisations. Direct IT security spending ranged from 2% to 10% of total IT spend in the companies researched. But chief internet strategy officers estimated incremental activity driven by security requirements at between 2% and 25% of total IT spend. In general, insurance and healthcare executives believe they spend too little on cybersecurity. Banking and high-tech executives say their spending on cybersecurity is about right.

Partnering with the public sector

The public sector has a responsibility to employ adequate means in order to address the growing cyber threat. As such, cyber resilience should be made part of relevant policies or systems such as a national cyber strategy, an end-to-end criminal justice system, and laws for the public good.

- *National strategy*: lack of national coordination can lead to redundant policy and legislation, thereby hindering economic growth and development. A comprehensive and transparent national cyber strategy that is integrated and harmonised with the strategies and procedures across the whole spectrum of domestic and international policy might constitute the right response. It is also important that such strategies incorporate the private and civil sectors, as well as leverage economic and security issues, among other tools, to drive the adoption of initiatives. Furthermore, a competent institution is needed to be responsible for the successful implementation and roll-out of the national strategy. An identifiable, responsible institution will offer transparency to stakeholders in the process. Not having a clear interlocutor to consult often leads to challenges of ownership, function and action, the research highlighted.
- *End-to-end criminal justice system*: Law enforcement needs to have the capability and resources to investigate cybercrimes and to have an appropriate, comprehensive and agile legal code to support its investigative and prosecutorial activities. Cyber resilience is a complex matter that may not be entirely clear to everybody in the criminal justice system. As such, it is critical that legal advocates, either through further education or other training, understand the cyber resilience ecosystem well enough to carry out due process.

- *Public good*: For the public good, all stakeholders need to ensure that they contribute to and maintain an evolving and robust incident response capability. This ranges from established programmes for information sharing and incident response such as CERTs (Computer Emergency Readiness Teams), to information training and development of human resources. Such a dynamic approach demands an ever-evolving set of capabilities to match the changing pace of the threat. Maintenance includes possible funding for cyber resilience research and greater investment in cyber resilience technical education in order to foster a more cyber-aware workforce.

Box 2: Partnership for Cyber Resilience

The Partnership for Cyber Resilience, launched at the World Economic Forum Annual Meeting 2012 in Davos, Switzerland, aims to help build cooperation and improve global cyber resilience. In 2013-2014, a joint effort was conducted between the World Economic Forum and McKinsey & Company to assess the necessary action areas, and examine the impact of cyberattacks and response readiness. The Partnership identified three vital areas of robust cyber resilience: information-sharing, critical infrastructure protection and policy development. It draws on knowledge and opinions derived from a series of interviews, workshops and dialogues with global executives and thought leaders.

The Partnership for Cyber Resilience recognises the interdependence of public and private sector organisations in today's global, hyperconnected environment. Companies participating in this community-led initiative understand the importance of integrating cyber risk management into their day-to-day operations and of sharing information on threats and vulnerabilities. As part of its multistakeholder dialogue across regions and sectors, the Partnership for Cyber Resilience also accepts that no static, universal set of actions can address the rapidly evolving environment of cyber risks. A framework was developed to prompt the discussion about the necessary steps to improve cyber resilience and to spur cooperation in building a stronger cyber resilience ecosystem.

The latest work, conducted under the umbrella of the Partnership, has shown that a range of high-value responses exists upon which a vigorous cyber resilience capability can be built at the institutional level. This group of institutional readiness responses comprises governance issues, programme development and network expansions for private-sector institutions. On the one hand, these responses address an immediate need of executives for specific steps to shore up their companies' current cyber resilience capabilities and establish critical benchmarks. On the other, the responses may form the core of a cyber resilience model that, over time, can foster companies' collaboration with partners in public and international policy, as well as community and systemic responses.

Source: World Economic Forum, *Risk and Responsibility in a Hyperconnected World, 2014.*

While advancing the efforts in the abovementioned areas, one cannot ignore the debate about the need for accountability and liability. Voluntary adoption of standards and norms or incorporating a transparent risk management approach

is one way to introduce accountability. Alternatively, governments may choose to set the standards and ensure liability which may result in regional diversification and consequently imply additional costs for companies. It is also important to keep in mind that as organisations determine who will assume the liability of the hyperconnected relationship they share, any unexpected or catastrophic financial or legal event has the potential to disrupt innovation and growth.

What next?

In cyber resilience components where public and private interests intersect, it is vital for the community to agree and act as one. This is particularly important for infrastructure, which often accommodates many interests. A rapidly changing cyber resilience landscape requires all government mechanisms to support the efforts of law enforcement and to be appropriately agile. A series of actions can greatly improve the quality of conversation on cyber resilience and accelerate coordination. Although thinking on this issue continues to evolve, two areas offer promise in building maturity in the ecosystem:

- *Risk markets*: Making use of a developed cyber risk insurance market to trade and monetise the risk from cyber events. Cyber-risk markets can distribute and offset some of the risks that cyber events present. Although the debate about pricing and policies still continues, the potential benefits can be big for many businesses.
- *Embedded security*: Exploring options to embed security parameters earlier into the lifecycle of products, and even into contemporary means of communication, such as the internet. Often, security is incorporated as an add-on to product, rather than from the onset.

Against this backdrop of high-value responses, it is worth noting that another range of actions is likely to deliver low or uncertain value in fostering cyber resilience. For example, while governments may be in a position to disrupt supply chains for attack vectors, such a move by private sector institutions would seem to be uncertain or counter-productive because of the collateral fallout. All of this reiterates the need for a collaborative approach to address cyber risks.

Cyber resilience or cybersecurity is still a fairly nascent topic, and requires further investment from interested parties to be fully understood and developed. As such, it is important to encourage public and private sector efforts to better understand the impact of cyber resilience on enterprises, nations and macroeconomics. Private, public and civil dialogue is needed to develop a coherent mix of policy and market mechanisms for use in the cyber ecosystem (see Box 3). Not taking a multistakeholder approach risks eliciting a mix of responses that could be weighted unevenly in one area, resulting in limited success.

Box 3. Selected recommendations from *Risk and Responsibility in a Hyperconnected World (2014)*

Governance
- Prioritise information assets based on business risks
- Integrate cyber resilience into enterprise-wide risk management and governance processes
- Lead in practice and policy from top leadership

Programme/network development
- Provide differentiated protection based on importance of assets
- Develop deep integration of security into technology environment to drive scalability
- Deploy active defences to uncover attacks proactively
- Continuous testing to improve incident response
- Enlist front-line personnel – helping them understand value of information assets

National cyber strategy
- Have a comprehensive national cyber strategy integrated with other policy domains
- Strategies should encompass economic and security issues
- Establish a competent institution for the national strategy implementation and rollout

Domestic policy and incentives
- Private, public, and civil dialogue to develop coherent mix of policy and market mechanisms
- Governmental mechanisms support law enforcement efforts and are appropriately agile

Foreign policy
- Establish a national cyber doctrine
- Identify persons at the local and national level responsible for cybersecurity
- Establish formal and informal channels of communication between law enforcement entities
- Work to harmonise policies surrounding the prosecution of cybercrime
- Establish a multi-stakeholder approach towards governance on this issue

Public good
- Ensuring evolving and robust incident response capability
- Increase investments in cybersecurity technical education
- Fund a cybersecurity research agenda
- Provide 'safe harbour' protection for limited sharing of information among and between companies and government

Research
- Increase education and awareness
- Encourage research on enterprise and the macroeconomic impact of cybersecurity
- Create an atmosphere in which white-hat research is encouraged

Shared resource for capability building
- Foster partnerships between governments, universities and the private sector for skills development

Information sharing
- Improve the quality of the ISACs/ CERTS/ CIERTs and other information sharing venues
- Promote an interoperable, extensible and automated system for sharing
- Provide common protocols to share information regarding cyber events

V. CAPACITY BUILDING AS A MEANS TO COUNTER 'CYBER POVERTY'

Enrico Calandro and Patryk Pawlak

The importance of Information and Communication Technologies (ICT) for development was acknowledged at the World Summits on the Information Society that took place in Geneva (2003) and Tunis (2005). At both meetings it was recognised that the diffusion of new technologies opens new possibilities of empowerment for the poor by providing them with access to various services such as banking and health information, which otherwise they would have difficulty accessing. The focus on the contribution that the internet and ICT make to growth and jobs creation around the world – largely attested in the Millennium Development Goals – has become even stronger in the aftermath of the global financial crisis of 2008. The ability of a country to drive competitiveness through technological development is regularly addressed in the *Global Information Technology Report* or more specific reports focusing on the contribution of the internet to national GDP. For instance, the analysis of 13 large economies conducted by the McKinsey Global Institute (2011) has shown that the internet accounted for, on average, 3.4% of their GDP and the creation of 2.6 jobs for one lost. The same study showed that the internet's total contribution to global GDP is bigger than the GDP of either Spain or Canada, and that global internet-driven GDP growth is greater than that of Brazil. At the same time, the dark side of ICT – in terms of the ethical, societal, economic and security risks associated with their use – has remained under the radar screen of both development and security communities. However, taking into account such risks and their negative impact on development, it is clear that policymakers need to reflect upon the possibility of the emergence of a new type of cyber-related poverty and exclusion. Although access to internet and mobile technology in developing countries is improving and the benefits offered by ICT are increasing, neglecting security and resilience measures can undermine and reverse this trend, affecting citizens and businesses. Consequently, the discussion about 'cyber poverty' traditionally understood in terms of the digital divide needs to take into account risks in cyberspace. As the international community prepares to decide on the post-2015 development goals, elements of ICT policy and technical resilience should feature as a new measure of development in the relevant discussions.

Growth in cyberspace

With ICT becoming the largest distribution platform for providing services around the globe, new opportunities are becoming available in terms of health, education or trade services to millions of people, in particular in remote areas. This also

translates into higher growth rates. According to the World Bank report *Building Broadband: Strategies and Policies for the Developing World (2010)*, in low- and middle-income countries every 10% increase in broadband penetration accelerates economic growth by 1.38%. Broadband access improves business productivity, supports the development of new products and services and boosts innovation. Direct economic impacts of broadband deployment include jobs created by rolling out broadband infrastructure, and indirectly it has 'spill-over' consequences such as increased productivity and new products and services. The World Bank's ICT4D 2006 report covering 20,000 firms from 26 sectors in 56 developing countries concluded that businesses making extensive use of ICT (phone, PC, email) are more productive and more profitable due to better management. There are also examples demonstrating how limited access to internet and ICT services in general impacts adversely on the economy. Following the ethnic riots in the Chinese province of Xinjiang in 2009, the regional government put it on electronic lockdown: internet access and SMS messaging services were blocked and international direct dialling (IDD) services were suspended. As a consequence, more than 6 million internet users were cut off from the rest of China and the world – a move that translated into a steep fall (44%) in Xinjiang's exports.

At the same time, one cannot ignore the importance of creating the right policy and legislative environment for ICT roll-outs and reforms in specific policy areas that would enable citizens and businesses to take full advantage of ICT. According to the World Bank, the implementation of ICT-related reforms in low-income countries generated investments worth US$16 billion between 1997 and 2006. However adverse effects may be observed if such reforms are neglected. In India, the e-Choupal model launched in 2000 leveraged the internet to link small farmers directly with buyers (see Box 1). But the expansion of this model has been delayed due to stalemates in market reforms, in particular concerning the Agricultural Produce Market Committee (APMC) Act which regulates fruit and vegetables markets that are governed by distinct regional committees. In addition, the discussion about ICT for development needs to reflect different objectives of specific countries and regions. For instance, while access to ICT remains a key challenge in several African countries, Asian states focus on knowledge-based economic development and reaching high-income status through investment in ICT, research and education. Given those different priorities, the overall development and poverty reduction strategy should guide ICT planning and implementation in order to address the specific needs of a country or a region, not only in terms of improving access to and use of ICT, but also in order to develop policy and regulatory capacity to effectively stimulate and facilitate the market to function properly.

Box 1: The enabling role of information: e-Choupal in India

The big potential of agribusiness in India is undermined by structural elements like fragmented farms, weak infrastructure and involvement of numerous intermediaries. Indian farmers have also been trapped in the vicious circle that has reduced their competitiveness: low risk-taking ability translates into low investments which results in low productivity and together with weak knowledge of the market results in low value added and low margins. That in turn reinforces the low risk-taking ability.

e-Choupal was launched in 2000 to improve the efficiency of the supply chain within the Indian agricultural sector by using ICT and quickly became the largest internet-based intervention initiative in rural India. Today, e-Choupal services are provided to over 4 million farmers through 6,500 kiosks in over 40,000 villages across ten states – ranging from smaller states like Haryana to bigger ones like Tamil Nadu, Rajasthan or Madhya Pradesh.

The real time information and customised knowledge delivered by *sanchalaks* – village internet kiosks managed by farmers and providing information (in the local language) about the weather, farm practices and risk management and connected to the mandi system for price discovery – enable farmers to take informed decisions about their businesses and align their production with market demand. The model benefits both farmers and bigger businesses like exporters of agricultural commodities (e-Choupal was conceived by ITC's Agri Business Division) and also reduces the transaction costs by providing the former with direct access to information about prices and the latter with the lower net cost of procurement.

Source: ITC website and press.

Security risks in cyberspace

The transformational power of ICT as a facilitator in delivering new solutions to traditional development challenges can be easily undermined if risks associated with these new technologies – mobile and internet tools particularly – are not properly addressed. The Busan Partnership for Effective Development Co-operation of 2011 stresses the importance of strengthening resilience and reducing exposure to shocks, especially in highly vulnerable settings such as small and developing states. As stated in the document, 'investing in resilience and risk reduction increases the value and sustainability of development'. In a similar vein, the World Development Report 2014 entitled *Risk and Opportunity: Managing Risk for Development* highlights the fact that hard-won social and economic gains can be jeopardised if systemic risks are not addressed by improving resilience defined as 'the ability of people, societies, and countries to recover from negative shocks'. The increasing complexity of computer systems requires accepting the fact that there is no absolute security and that in the event of a risk materialising, the information system or network will be able to rebound and continue to operate. Consequently, the infrastructure rollout programmes and

regulatory frameworks aimed at strengthening the impact of ICT on economic and social development need to be increasingly accompanied by the simultaneous adoption of adequate risk management strategies. The need 'to foster confidence in information systems' as a fundamental requirement for economic and social development stemming from ICT was addressed already in the OECD *Guidelines for the Security of Information Systems* adopted in 1992. The digital security risk management framework currently being discussed at the OECD emphasises the risk-based approach to security and the shift from the protection of information systems and networks to the protection of the economic and social activities that these systems and networks support.

Box 2. Role of ASEAN in building resilience in Asia

In 2003 the ASEAN Telecommunications and IT Ministers Meeting (TELMIN) adopted the Singapore Declaration that highlighted efforts to establish the ASEAN Information Infrastructure with a view to promote interoperability, interconnectivity, security and integrity. The Ministers decided that all ASEAN countries should establish national Computer Emergency Response Teams (CERTs) by 2005 in line with mutually agreed minimum performance criteria. The Framework for Cooperation on Network Security together with an Action Plan were adopted in Malaysia in 2005 and revised in 2013 at the 19th ATRC Meeting in Manado.

In addition, two of the six strategic pillars in the ASEAN ICT Masterplan 2015 (AIM2015) adopted in 2011 are explicitly related to cybercrime and aim at promoting secure transactions within ASEAN (Thrust 2: People engagement and empowerment) and push for a number of security-enhancing measures (under Strategic Thrust 4: Infrastructure Development) that promote network integrity and information security. These include for instance: establishing common minimum standards for network security, developing a network security 'health screening' programme for ASEAN, and establishing the ASEAN Network Security Action Council (ANSAC) – a multi-stakeholder initiative to promote CERT cooperation and sharing of expertise. The first meeting of the ANSAC was held on 5 June 2013

In July 2012, the ASEAN Regional Forum (ARF) issued a Statement on Cooperation in Ensuring Cyber Security which included a number of measures to intensify regional cooperation. For instance, the Statement recommends the development of an ARF work plan on security in the use of ICT that would, *inter alia*, advance strategies consistent with international law and encourage and enhance cooperation in promoting a culture of cyber security.

Source: Presentation by ASEAN representatives at the Octopus Conference, December 2013. Available at the Council of Europe website.

That also implies that issues concerning the safety and security of cyberspace in developing countries need to be located in their own specific internet ecosystem. Access to and use of voice and internet communications, institutional arrangements, technical and financial resources to regulate the sector, and often the way in which human rights frameworks are applied, are different in developing countries

compared to the global North. The International Monetary Fund (IMF), for instance, found that the increasing use of mobile phones across the continent contributes to financial inclusion and economic growth in Africa by facilitating access to relevant information and reducing transaction costs through, *inter alia*, the development of branchless mobile money transfer services (see Figure 1).

In order to understand the complexity of the challenge, it is necessary to assess the degree to which resilience and security of cyberspace is indeed a real problem. Trends in population growth and access to new technologies suggest that there will be a growing disparity between a device-rich North and people-rich South. For instance, mobile phone ownership in Ethiopia, Rwanda and Tanzania is very low and even in countries with better results, phones usually do not have features enabling users to browse the internet. Even in countries like South Africa where the percentage of mobile phone owners is relatively high (84.2%) only half of the used phones are capable of browsing the internet – a feature which is used by only 28% of owners. At the same time, research into individual internet use conducted by Research ICT Africa in 11 African countries suggests that a majority of the population has used the internet for the first time on their phone (e.g. 70% of Ugandan and 67% of Ethiopian internet users). That implies that security challenges are different to those typical for countries where the internet uptake is more common. With a growing number of mobile subscriptions – estimated at more than 8 billion in 2013 – mobile phone users have increasingly become the targets of cyberattacks feeding the lucrative criminal industry to the tune of an estimated USD 50 billion (see Box 3). An increasingly common practice is mobile caller ID spoofing – or 'phone phreaking' – a type of phone hacking that uses software or technology to display on the person's caller ID a number different than the original one.

A comparison of the development and cybersecurity agendas also suggests some clear overlapping objectives, including respect for rule of law, promotion of human rights and good governance. For instance, a rights-based approach in development cooperation can benefit significantly from the frameworks promoting the protection of human rights offline and online. In that sense, underdeveloped frameworks for privacy and data protection are another serious problem in developed and emerging economies. For example, the case of inBloom – a project aiming at developing personalised teaching methods for pupils using their personal data gathered on tablets – shows that initiatives potentially contributing to personal development can be derailed by opposition from parents if no adequate safeguards are in place.

Development agencies also recognise the key role of the private sector in achieving poverty reduction by providing employment, investment and stimulating innovation. This thinking is shared by the cybersecurity community which considers private sector actors (i.e. IT companies, telecommunication firms, etc.) as key stakeholders in building secure and resilient systems. At the same time, both communities are concerned with the transparency and accountability of the private sector, in particular in terms of respect for human and labour rights, safeguarding citizens' and children's rights, etc.

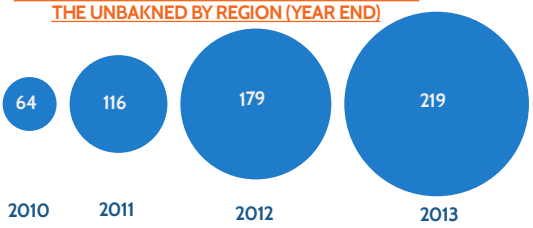
Figure 1. Closing the financial infrastructure gap with ICT

The rollout of ICT in Africa has had 'a leapfrogging effect' on the infrastructure, resulting in growing mobile phone penetration and coverage. Even though formal bank services are the most popular financial system, the growing use of mobile phones has contributed to reducing the financial exclusion of large numbers of the population: 78% in Mozambique and 62% in Uganda. It is estimated that in 2010 about 2.7 billion people in low- and middle- income countries were unbanked. The examples of existing services include:

- M-PESA by Safaricom (Kenya)
- M-KESHO by Equity Bank and Safaricom (Kenya)
- MTN MobileMoney by MTN (Benin, Cameroon, Côte d'Ivoire, Ghana, Guinea Bissau, Nigeria, Rwanda, South Africa, Swaziland, Uganda, Zambia)
- Easypaisa by Telenor (Pakistan)
- Mobile Money by Tigo (Tanzania, Rwanda, Ghana, Paraguay, El Salvador, Guatemala, Honduras, Bolivia)

According to the State of the Industry Report 2013 published by Mobile Money for the Unbanked, mobile money is available in most developing countries, providing 219 services in 84 countries. The importance of this service is confirmed by the fact that 70% of providers plan to increase their investment in mobile money in 2014. The competition on the market is already increasing with 52 markets already having two or more mobile money services.

NUMBER OF LIVE MOBILE MONEY SERVICES FOR THE UNBAKNED BY REGION (YEAR END)



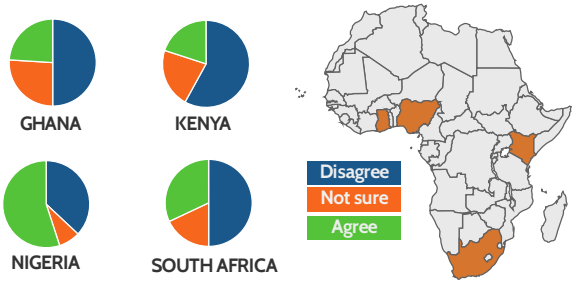
98.3 million registered accounts/42.4 million active accounts

35.5 million registered accounts/10.5 million active accounts

8.3 million registered accounts/2.4 million active accounts

A few factors specific to the Kenyan context contributed to the success of MPESA. First, it was driven by Safaricom, the dominant mobile operator with considerable market share in the Kenyan market; second, no licence to provide the service was required by the Kenyan regulator; and third, the financial market in Kenya failed to provide services to the segment of unbanked.

USING TECHNOLOGY IS RISKY, TECHNOLOGY MAY FAIL



Issues around trust, safety and security of mobile money transfer have been investigated by Research ICT Africa which has explored whether mobile money transfer is perceived as safer than other means of sending or receiving money in selected African countries. Overall, from survey results it emerged that mobile money transfer is perceived as safer except in Rwanda, Ghana and Namibia, where it is considered as safe as other services. Likewise, in most African countries surveyed by Research ICT Africa, mobile money transfer is perceived as more trustworthy. In addition, the technology is not considered risky by mobile money transfer users.

Source: Mobile Money for the Unbanked; Research ICT Africa 2012

Box 3: The cost of non-security: mobile caller ID spoofing

The case of M-PESA – a mobile money transfer system created by Vodafone with its African subsidiary Safaricom – demonstrates how the provision of new services by a company may expose it to attacks by cyber criminals. One of the agents providing the service has lost as a consequence €340 – an insignificant amount for a European citizen but the equivalent of 27% of per capita GDP and a capital loss that it would take an average Kenyan over 18 months to replace. In 2013, mobile money agents in the central region of Kenya lost about USD 13,000 a month due to caller ID spoofing. The strategy boils down to a combination of regular fraud and the exploitation of the telecom service provider. The perpetrators claimed to work for Safaricom – the service provider – and convinced the M-PESA agents to provide them with detailed information about their businesses, including the agents' ID number and PIN. In response, some companies have launched telephone transaction platforms that help to validate caller identities (e.g. TrustID.com). Mobile money transfer agents in Kenya have formed the Association of Mobile Phone Money Transfer Agents of Kenya (AMPHOTRAK) with the aim to educate members on the most recent trends in mobile fraud.

Source: Online press reports.

The discussion about ICT for development also needs to take account of potential inequalities and distortions that emerge as a result of such programmes and abuse of the most vulnerable groups. Numerous press reports contain stories of low-paid workers in developing countries who deliver Facebook likes, YouTube video views and Twitter followers – working on a three-shift system and paid as little as €100 a year.

The fight against corruption is another useful example that could bridge the two communities. Corruption distorts decisions about the provision of public services such as education and healthcare which can fuel social and political grievances. It also provides a space whereby institutions are exploited for private gains. This is an important element in the context of research into the transparency and openness of donor countries and aid agencies. With a growing market for ICT technologies but also for cybersecurity assistance, it is therefore important to limit any abuses, in particular during the procurement processes. New anti-corruption legislation was introduced in several markets, in both large and small economies. Brazil's 'Clean Company Law' prohibits engaging in or attempting bribery of foreign and domestic officials; the Lokpal and Lokayuktas bill in India created the position of Ombudsman to investigate allegations of corruption. In Zambia, for instance, key anti-corruption institutions were set up with the support of the donors.

Fighting cyber poverty with human resilience

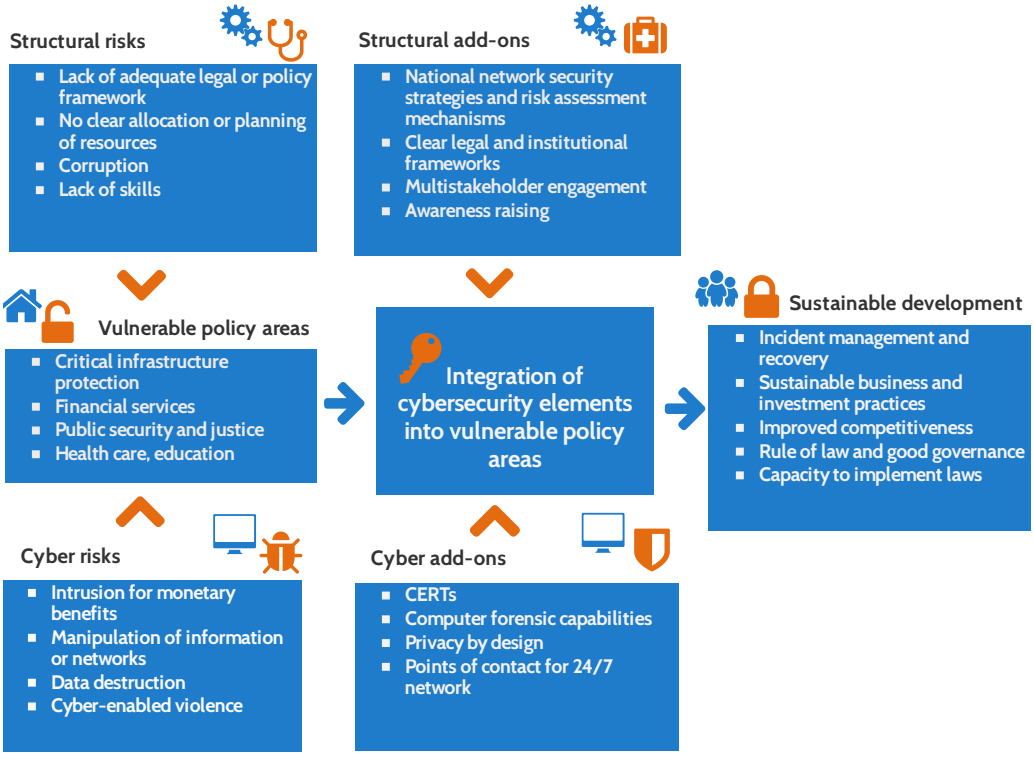
Challenges to development and the ICT environment can be partly addressed with capacity-building initiatives that improve resilience and mobilise all stakeholders. In that context, the concept of human resilience (i.e. 'ensuring that people's choices are robust, now and in the future, and enabling people to cope and adjust to adverse effects') introduced in the *Human Development Report 2014* is particularly helpful. This aim can be achieved by putting in place the right institutions, structures and norms. Numerous lessons for cyber capacity-building can be learned from the development community. Two decades of engagement in ICT projects indicate problems with the ICT4D approaches: technology dumping, investment in infrastructure without capacity building, failure to recognise the impact of regulatory frameworks, and the lack of analytical background for mainstreaming ICT into specific development areas like education, access to water or electricity. Some studies also stress the distortive effects of ICT projects on other areas of development. For instance, the share of household income devoted to mobile services is rising which reduces the budget for food, health or education.

Furthermore, a response should be tailored to the situation on the ground, for instance taking into account the low level of internet penetration in certain countries. In countries like Ethiopia, Rwanda or Mozambique the discussion about cybersecurity is difficult as they do not have adequate legislative frameworks in place. In some African countries the idea that respect for human rights, democracy and the rule of law can serve as a basis upon which specialised areas of cyber-law can be developed is simply erroneous. The situation is further complicated by the fact that generally there are limited technical capacities and resources at a regulatory level. According to the United Nations Economic Commission for Africa (UNECA), African governments are demonstrating increasing awareness of cybersecurity issues, but existing capability to deter cybercrime and monitor or pursue cybersecurity has been ineffective. Also, cybersecurity concerns in response to a widespread diffusion of mobile connectivity have been often addressed in concomitance with privacy and surveillance implications in Africa, and at the moment are largely overlooked. For instance, one of the key aspects of Africa's emerging mobile-centric surveillance society is the rise of SIM registration requirements. These are now in force in the majority of African countries, and have a range of implications for inclusion, surveillance, and development. On the other hand, it would be irresponsible to dismiss increasing security concerns and potential risks. Although African states have not yet achieved a high level of digitalisation this does not imply that they are not vulnerable to the new forms of threats that exist in cyberspace.

Therefore, it might be more accurate to address challenges in cyberspace from the risk management perspective with its diverse policy responses, including technological adaptations, legislative framework, and institutional arrangements. At the same time, given the speed with which technological progress is occurring, it is important

to think of capacity building as a dynamic process whereby the needs of concerned stakeholders are in constant evolution. Mainstreaming various structural and cyber-specific 'add-ons' into different policies may result in the development of policies that are more resilient to all types of risks (see Figure 2). For instance, the predominantly security-based approach adopted by some countries risks becoming unsustainable and costly – hence undermining the benefits for society and the economy – if the overall approach to cybersecurity does not address structural risks (e.g. no clear allocation of resources) or if proper risk assessment mechanisms are not put in place. Another useful example is the protection of critical infrastructure where in order to improve the security of the most important infrastructural services (i.e. energy, transportation, the supply chain) there is a clear need to include elements that will enhance cyber resilience (i.e. CERTs, points of contact) in a broader framework that also includes legal and personnel aspects.

Figure 2: Integrating cybersecurity into other policy areas



VI. MODELS FOR CYBERSECURITY CAPACITY BUILDING

Patryk Pawlak

Introduction

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, there has been an increasing emphasis on addressing digital security risks as a precondition for the overall success of investments in the development of ICT infrastructure and other projects with an ICT component. The risks vary from attacks targeting individuals (i.e. phishing, mobile spoofing) to more sophisticated threats against society at large (i.e. attacks on critical infrastructure, like energy and water networks) or governments (i.e. data breaches, DDoS attacks). Dealing with this new reality first requires acknowledging that development objectives and risks related to the digital environment are two sides of the same coin, and 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, and exchange best practices and lessons learned. Achieving this aim is not an easy task and is usually conditional on several important decisions concerning: (i) a concrete goal to be achieved and identification of the relevant actors to be involved; (ii) the definition of digital security risks and a method for mainstreaming risk management elements into a cooperative enterprise; and (iii) a format that guarantees the most effective engagement between different actors.

Content and membership: who is in, who is out?

Membership – defined as a formal belonging to or a loose association with a specific group – is one of the key elements determining the success or failure of any capacity-building effort. This is related to the fact that decisions about participation in a specific endeavour are based on such aspects as similarity of views or goals (e.g. between security and development actors), the distribution of resources destined for a specific initiative (e.g. financial, human, etc.), access to the decision-making process, including voting rights (if applicable, usually only in formally organised organisations) and, ultimately, trust. Therefore, a decision about who to cooperate with and to what extent is a strategic one and has an impact at the level of individual commitment towards collectively established objectives.

In the case of cyber capacity building, a coherent narrative about its objectives is still missing. One clearly identifiable strand of reasoning attempts to mobilise stakeholders by invoking the economic costs incurred by a weak cybersecurity framework. Consequently, advocates of this viewpoint support the focus on protective measures and the fight against cybercrime. Another narrative is constructed around the link between the security of cyberspace and social and economic development. The underlying assumption here is that the expanding use of ICT for development needs to incorporate security elements in order to support economic growth and sustainability in the future.

One of the key challenges for cyber capacity building in this respect is to bring together actors with different organisational cultures and objectives, and build a constructive relationship between them. That implies a decision about who to include in – and who to leave out of – a specific initiative. While homogeneous groups (those bringing together members of the same community, e.g. diplomats, technical experts or development actors) increase cooperation between their members, heterogeneous networks bringing together diverse actors (e.g. cyber experts, diplomats) often prove to be more difficult, especially when limited trust between members raises doubts about the objectives of a given group. Although maintaining relationships within homogenous groups is resource-intensive and time-consuming, and the result is less prone to generate innovative approaches, it is also more likely to stimulate in-depth two-way communication and the exchange of detailed information and consequently be more successful in deciphering the implications of external threats. This is one of the reasons behind the emergence of several informal transgovernmental networks, including those linking cybersecurity experts. An incentive to diversify the community may be, for instance, the need to acquire new resources – i.e. legal authority, organisation, funding, expertise, information and experience – that are currently spread across many different organisations.

Multistakeholder approaches involve a diverse array of actors and thus expand membership beyond governments. But for such an approach to yield results, the main objective around which specific initiatives are developed needs to be clear and the *entire* community of stakeholders brought together (i.e. government, industry, local councils). The experiences of numerous countries (e.g. Nigeria, Kenya, Ghana and Pakistan) demonstrate the multiple benefits of cooperation between stakeholders: it has an energising effect, ensures better capacity, and results in more inclusive outcomes with greater perceived legitimacy. It also helps promote good governance (e.g. the Sri Lankan CERT and Central Bank Payment System).

Box 1. Membership matters: examples of cyberspace governance in Africa

Due to limited capacity and resources several African regional economic communities and national governments have increased their dependence on inter-governmental organisations in terms of agenda setting but also implementation. Specific aid programmes and technical assistance – backed with a financial envelope – have increasingly gained in importance and opened the gates to international organisations.

The International Telecommunications Union (ITU) is considered by many as the preferred option to address challenges related to physical infrastructure, the definition of technical standards and services and other issues concerning the internet. This can be explained through several features of the ITU itself, including the intergovernmental approach and nation state membership as well as restriction of active participation to member states.

Significant efforts have been also made by the African Union and its eight Regional Economic Communities (RECs) – Arab Maghreb Union (UMA), the Common Market for Eastern and Southern Africa (COMESA), the East African Community (EAC), the Economic Community of Central African States (ECOWAS), the Intergovernmental Authority on Development (IGAD), and the Southern Africa Development Community (SADC) – who are strategic partners in the implementation of the New Partnership for Africa's Development (NEPAD). The complexity of the African regional architecture is further increased by additional regional economic cooperation bodies which are not recognised by the African Union.

Even though regional organisations are tasked to coordinate, harmonise and integrate national policy and regulatory frameworks, these roles are often difficult to accomplish. Some of the most common challenges include the need to manage confusion and competition caused by multiple and overlapping memberships, operating in a resource-strapped environment with limited financial and human resources and the non-binding nature of requirements which makes effective compliance even more difficult to achieve. Under such circumstances, acquiring membership in networks with expertise and resources is a very attractive solution providing access to technical and financial support from international organisations like the ITU, World Bank, the European Union or the Council of Europe.

Source: Calandro et al. (2013)

Method: isolation, cherry-picking and integration

With the growing application of ICT in various spheres, it is important to look into methods for mainstreaming digital security risk management across a range of policy areas including agriculture, energy, transportation, education and health. Although specific risks and challenges for each are different, it is imperative to take into account various aspects of cybersecurity across the board. Even though there is no 'one size fits all' solution to cybersecurity problems, and no single cyber capacity-building model, certain elements can be universally applied while recognising the specificities of a

cultural, political and social context. For instance, even though responsibilities can be assigned differently depending on the country in question, functions often remain comparable.

The experiences thus far with mainstreaming cybersecurity elements into other policy areas help to distinguish different phases of that process, which may be broken down broadly into the following categories: (i) isolationism; (ii) cherry-picking and (iii) integration. The first is primarily associated with the so-called 'silo mentality' whereby each policy community focuses on its own mission and objectives, eventually leading to compartmentalisation. Consequently, the consideration of digital security risks is not integrated into broader policy discussions. This has been the case so far for many ICT development projects but also in the realms of energy and transportation infrastructure.

The second method, cherry-picking, implies that cybersecurity elements are conceived *ad hoc* in the context of specific projects or as one-off collaborative efforts. These are often temporary 'coalitions of the willing' between different actors (in both the public and private sectors) rather than systematic endeavours. That does not mean, however, that they cannot evolve into longer-term cooperation. For instance, the ongoing cybersecurity cooperation between the European Union and the Council of Europe remains limited to combating cybercrime through cooperation between law enforcement agencies with the funding provided by the European Commission's Directorate for Development Cooperation. Similarly, alliances of like-minded donors that are currently being pursued in the form of joint programmes would qualify as cherry-picking as they focus on specifically selected issues.

Lastly, integration is the most systematic and enduring way of bringing digital security risks into and across other policy areas – even though it presents the most challenges. The main difference between cherry-picking and integration methods is the creation of an explicit and enduring link between cybersecurity and other policy areas. For instance, an initiative with the objective of enhancing cooperation on resilience of critical infrastructure protection would not be considered as integration *per se* unless it became a part of the agenda in other policy areas like energy, telecommunications, etc. At best, integration promotes the harmonisation and streamlining of activities and procedures to avoid duplicative efforts and to share practices. Most of the time, attempts at integration take the form of informal networks in order to allow for speedy and inclusive knowledge sharing among a broad circle of stakeholders.

Format: hierarchy and networks

Relationships between actors can usually be arranged as hierarchical structures or networks – both serving different purposes. Hierarchical structures – typical of international 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 decreases – primarily due to the absence of adequate resources (usually in the possession of other actors not directly linked to any part of the existing hierarchy). In those cases, the structure most often evolves into a networked one.

Several features of networks seem to be of particular relevance for cyber capacity building. First, networks provide space for a 'peaceful' clash of ideas that result from different – sometimes conflicting – interests. Despite such elements of tension, the high intensity of interactions stimulates learning processes between members of the network and ultimately may be conducive to building trust. Naturally, shared values and worldviews provide a good basis for developing trust but are often absent whenever security issues are in question. Second, networks provide a stronger basis for addressing uncertainties related to specific challenges by bringing diverse actors to the same table and hence provide better access to resources (i.e. information, funding, etc.). This is particularly relevant for capacity-building projects which rely on effective mechanisms for the diffusion of information, dissemination of ideas, and innovation.

With regard to actors, the role that specific government entities (i.e. ministries or separate government institutions) play in the policy-making process at the domestic and the international level needs to be acknowledged. That is of particular importance in the cybersecurity context where responsibilities are distributed among different parts of an administration with organisational cultures of their own which then reflects on the dynamics within the group (e.g. ministries of defence may have a more hierarchical and defence-oriented focus, ministries of interior a law enforcement focus while the ministries of finance or telecommunications may favour a market-oriented approach).

What direction for cyber capacity building cooperation?

Although the importance of capacity building in cyberspace is increasingly acknowledged by governments, international organisations and the private sector, the proliferation of initiatives has led to obvious questions concerning the efficiency and sustainability of related efforts. This, however, brings to the fore another challenge, which is that of defining a strategic framework for capacity building that could unify multiple projects and initiatives. The absence of a coordinating mechanism that would help establish a broader picture of capacity-building efforts raises serious problems for both donors and beneficiaries: on the donors' side, it often leads to duplication of tasks and inefficiencies; on the beneficiaries' side, it leads to confusion with regard to objectives, conditions and motivations underlying efforts undertaken. The three dimensions mentioned above allow for distinguishing at least four models of cyber capacity building that have emerged around the world (see Figure 1).

Figure 1. Examples of various memberships: methods and formats

Example of a homogeneous group

The Meridian Process brings together governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally. The aim is to exchange ideas and initiate cooperation, explore the benefits and opportunities, and provide an opportunity to share best practices. Participation in the Meridian Process is open to all countries/economies and is aimed at senior government policy-makers involved in CIIP-related issues.

Example of a heterogeneous group

The Global Partnership brings together representatives of 161 governments and 56 business and civil society organisations around the issue of ending poverty. Created at the Fourth High-Level Forum on Aid Effectiveness in Busan, the Global Partnership complements the work of other organisations that impact effective development co-operation, including the Development Working Group of the G20 and the UN-led debate about the post-2015 global development agenda. The Global Partnership is uniquely inclusive (by bringing together diverse actors), open (it is a forum where developing countries, providers and others can air concerns and find solutions) and flexible (it has a rolling agenda).

Example of isolationist approach

The Forum of Incident Response and Security Teams (FIRST) is an international confederation of 305 trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programmes. Within the FIRST framework, Special Interest Groups provide a forum to discuss topics of common interest to the Incident Response community, with a goal of collaborating and sharing expertise and experiences to address common challenges. For instance, the Botnet Mitigation and Remediation Special Interest Group brings together FIRST members and non-members to identify different approaches and best practices that can be implemented to address this problem.

Example of a cherry-picking approach

Europol, the Organization of American States, FIS and Microsoft have signed memorandums of understanding to increase cooperation in the fight against cybercrime. This cooperation stems from the belief the collaboration will help strengthen their forensic and technical analysis of malware and botnets, improve the assessment and investigation of emerging malware threats, enhance the enforcement actions against cybercriminals and ultimately dismantle criminal organisations.

Example of integration approach

In order to achieve its objective of preventing, detecting and responding to threats to nuclear security, the International Atomic Energy Agency has started to include security of computer systems as one of the elements in its training programmes. In response to the potential threat to IT networks of energy facilities, the IAEA Department of Nuclear Security has initiated awareness trainings or advanced trainings in terms of IT/Cyber Security. The courses are delivered at national or regional levels. Main modules in the training programmes include computer security and access control, authentication and cryptography, computer security architecture, network security, intrusion detection and information recovery, and network management practices.

Example of a hierarchy

The Plenipotentiary Conference is the top policy-making body of the ITU where members decide on key issues related to the future of the organisation . The decision-making process at the conference has been criticised for its limited transparency and oversight. It remains very much state-centred, even though the ITU has made an effort to involve representatives from academia, non-governmental organisations and the private sector in its various activities. While private sector representatives may attend the plenipotentiary conferences to advise their respective governments, very few governments incorporate scholars or civil society representatives as members in their national delegations.

Example of a network

The Estonian Defence League's Cyber Unit (EDL CU) is a rare example of a diverse and open network mobilised towards the creation of a national culture of resilience. The EDL CU is a voluntary organisation with a mission to protect Estonia's information infrastructure and to support the broader objectives of national defence. The EDL CU brings together actors from key cybersecurity areas, including national critical infrastructure employees and specialists in other cybersecurity-related fields (e.g. lawyers, economists). The specific aims of the organization include, among others, facilitation of public/private partnerships as well as improving operating capacities if and when a crisis occurs.

Sources: Information provided on websites of respective organisations.

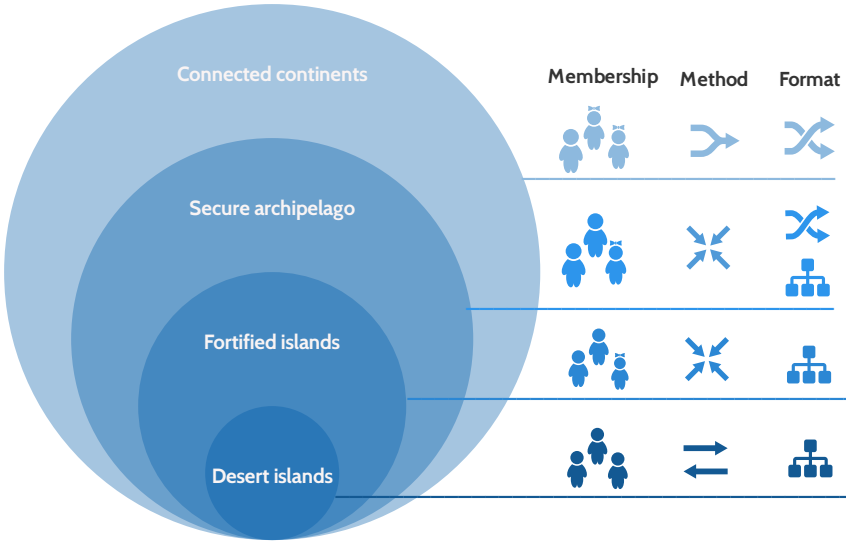
In a *desert islands model*, cyber capacity building is undermined by varied (and sometimes conflicting) policy objectives, organisational interests, and often limited knowledge about the scope of digital security risks in a given policy area. Consequently, each policy community focuses on capacity-building initiatives in accordance with its mission and pre-established policy objectives. Cooperation occurs primarily between members of the same community with very little or no communication with potential external partners, resulting in misconceptions, limited trust, and insufficient knowledge about initiatives undertaken by other networks. This may lead to suboptimal outcomes stemming from the duplication of efforts or repeating work that has already been done.

The *fortified islands model* assumes *ad hoc* cooperation between different groups whereby cybersecurity elements are addressed on a case-by-case basis depending on the issue. The impulse for cooperation comes from the need to address a complex problem which requires resources – financial, knowledge or otherwise – beyond the capacity of one specific group. It is possible that 'fortified islands' evolve into 'secure archipelagos', primarily as the outcome of functional spill-over. The main factor that explains the increasing adoption of this model is a growing awareness of the negative impact that the exploitation of vulnerabilities in cyberspace may have on the attainment of goals in other policy areas. This model of cyber capacity building has been implemented by the International Atomic Energy Agency in its training programmes where IT security features as a part of the curriculum.

The *secure archipelago model* represents situations where interactions between different communities take place on a regular basis but are still limited to a carefully selected set of issues. The continuity and regularity of cooperation is a key difference compared to 'fortified islands' which conceptualise security as an 'add-on' to their activities rather than an integral element. This is probably the most widespread model of cooperation whereby coalitions are established in order to resolve specific policy problems permanently. Such initiatives are usually expected to continue in the future and aim from the outset at making cyber-related issues a key part of their cooperation. Cooperation between the Council of Europe and the European Commission on the implementation and promotion of the Budapest Convention is an illustration of this model of cyber capacity building.

The *connected continents model* represents the most comprehensive form of cooperation. It ensures both the diversity of actors (which helps to ensure adequate access to resources) and shared commitment to mitigating digital security risks as an integral part of their efforts towards achieving their respective policy objectives. This could also be described as a comprehensive capacity development model whereby all members of a network contribute to a common objective. Even though the process may take longer than in other cases, it usually results in more solid and sustainable outcomes. The changes that were implemented in Estonia after a series of attacks in 2009 are a good example of how such an approach may function in practice.

Figure 2. Models of cyber capacity building



Identifying lessons for future cooperation

With regard to the cyber community, bringing together cybersecurity and development experts is particularly important. Given the growing importance of ICT for social and economic development, it is now essential to ensure that those benefits are not undermined by illegal activities in cyberspace. Unfortunately, the conversation is all too often dominated by misconceptions about respective objectives. References to cybersecurity – very often interpreted purely in military or law enforcement terms – are often politically loaded. This leads to problems with cooperation on concrete projects. However, any efforts to address risks to cyberspace presented in terms of their potential positive impact on good governance (i.e. transparency, legitimacy and accountability of government authorities and officials), human rights (i.e. the right to privacy) or economic freedom (i.e. online transactions, counter-corruption) have a much greater chance of bringing different groups together. This implies that the discussion about cybersecurity itself needs to be demystified in order to make it more accessible for other communities which either play an important role in shaping the overall policy or possess other substantial resources.

Learning and sharing

Different levels of technological advancement around the world suggest a wide scope of priorities – both for beneficiaries and donors depending on their specific interests. Therefore the discussion about the needs of specific countries must take

into account the local context – in terms of infrastructure, a regulatory framework, or a stage of implementation. It only seems natural that in order to facilitate this process, both donors and beneficiaries regularly exchange information about their progress, respective needs and priorities. Unfortunatelly, this is not the case and despite occasional meetings and initiatives, the exchange of information and sharing of knowledge is still lacking.

In their search for a model of international cooperation, both donor and beneficiary communities increasingly aim at identifying good and bad practices and improving information sharing on capacity-building efforts. This is important in order to identify needs, success stories and failures, and to better understand specific conditions that influence an outcome. The need for clarity when it comes to objectives is particularly of the upmost importance for many beneficiaries, especially in developing countries. As most of them struggle with numerous problems and limited resources, they need to carefully balance the immediate needs with long-term objectives. Regional organisations like the Organisation of American States (OAS), the African Union Commission, the Association of Southeast Asian Nations or the Council of Europe might be good channels for streamlining capacity-building efforts. The OAS, for instance, has recently launched its own study to identify the cybersecurity needs of its member states. Another interesting project is 'Cyber Green', launched recently by the Asia Pacific Computer Emergency Response Team network with the aim to establish an effective hub for collaboration efforts to address cyber risks and improve the health of the cyber ecosystem. However, each of these organisations also has its own limitations prescribed by the extent to which they share cultural values, language regimes (e.g. three dominant 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).

Resources (including political commitment)

Given limited resources and conflicting policy priorities, there is a temptation among policymakers to push cyber capacity building towards the bottom of the policy agenda. Already overloaded agendas of meetings and overstretched staff make the mainstreaming of cybersecurity issues very difficult. For instance, the Swedish International Development Cooperation Agency (SIDA) has undertaken a major effort to mainstream ICT into its development programmes in order to ensure broad commitment. After having tested a unit-led approach and mainstreaming they have eventually decided to establish in-house networks of experts with diverse backgrounds. Other agencies have explained the failure of mainstreaming due to insufficient political commitment.

In the light of the growing importance of ICT elements across numerous policy areas, the cybersecurity community has made a collective effort to improve policymakers' awareness of the adverse effects of insecurity. Consequently, building

security components into development programmes or law enforcement initiatives has become the preferred option for ensuring that cybersecurity concerns are taken on board in a systematic way. This approach, however, has been challenged by other policy communities who prefer to focus on their core business and either ignore security concerns or prefer to include them on an *ad hoc* basis. Myriad examples suggest that an exchange of experiences between various policy areas could be a fruitful and beneficial exercise. Several useful lessons could be potentially derived from other policy domains:

- Mainstreaming human rights into other policies has been broadly promoted by the OECD Development Assistant Committee (DAC). It seeks to systematically integrate human rights in all sectors of aid interventions. It extends the integration of human rights from traditional areas, such as governance and rule of law, to all areas such as energy, transport, the environment or health. This approach helps to ensure policy coherence and also includes safeguards that minimise the risk of unintended negative impacts of development activities contributing to human rights violations.
- Security sector reforms might serve as a good entry point for cyber capacity-building efforts due to their focus on core security actors (e.g. armies, intelligence and security services), security management and oversight bodies (e.g. ministries of defence, internal affairs), justice and law enforcement institutions (e.g. judiciary, criminal investigation and prosecution services) and non-statutory security forces (e.g. private security companies). The aim of these endeavours is to increase the ability of a state to meet the range of both internal and external security needs in a manner consistent with democratic norms and sound principles of good governance.
- The use of EU funds for cybersecurity-related objectives offers another example. The Instrument contributing to Stability and Peace (IcSP) focuses on technical and financial support in addressing threats to law and order, security and safety of individuals, and critical infrastructure. Assistance in those areas shall cover support for measures aimed at: strengthening the capacity of law enforcement and judicial and civil authorities involved in the fight against terrorism; organised crime, including cybercrime; addressing threats to critical infrastructure, which may include international transport, including passenger and freight traffic, energy operations and energy distribution, and electronic information and communication networks. The Partnership Instrument, on the other hand, supports cooperation measures with countries with which the Union has a strategic interest in promoting links, especially developed and developing countries which play an increasingly prominent role in global affairs, including in foreign policy, the international economy and trade, multilateral fora and global governance, and in addressing challenges of global concern, or in which the Union has other significant interests.

Coalition building

Several of the negative trends in cyber capacity-building cooperation could be reversed if appropriate management was put in place and existing structures were better connected. For instance, cooperation between development and security actors can result in a win-win situation whereby development objectives (i.e. human security) are achieved with the help of expertise from the cyber community (i.e. law enforcement agencies, etc.). Building coalitions also limits the danger of duplication of resources which are already scarce. For instance, aid databases to coordinate donors' individual commitments and disburse funds have been established in Mozambique, Indonesia, Cambodia and other countries. Another interesting example of how to deal with the multiple sources of funding comes from Indonesia's National Programme for Community Empowerment. According to the World Bank, the provision of investment resources to support productive proposals developed by communities, using a participatory planning process, proved to be an effective tool in improving local-level governance in rural areas and consequently reducing poverty. In line with the programme's objective, communities receive the funds and conduct participatory planning and take decisions determining their preferred projects and investments which are funded by both the government and a multi-donor trust fund.

ANNEXES

GLOSSARY OF CYBER TERMS

Advanced Persistent Threats (APTs): This term usually refers to the process of continuous computer hacking of a specific entity. APTs are particularly purposeful, resourceful and sophisticated.
Attack: An attack is an attempt to subvert or bypass a system's security. A cyber-attack is an attempt to damage a computer or system. Active attacks attempt to alter or destroy data. Passive attacks try to intercept or read data without changing it.
Back door: A back door is a feature programmers often build into programs to bypass normal authentication procedures. Programmers build back doors in programs in order to fix problems that arise at a later stage. However, back doors can pose security problems when hackers learn of their existence.
Big data: Large volumes of heterogeneous datasets arriving constantly from all kinds of connected devices which require advanced and non-traditional methods of processing, storage and analysis.
Botnets: A bot network is a network of computers that are hijacked and controlled by a hacker, through Trojan horses or other malicious codes. The network can be used to launch DDoS attacks.
Brute-force attack: A brute-force attack is an attack in which each possible key or password is attempted until the correct one is found.
Bug: A bug is an unintentional fault or flaw in a program that causes the program to behave in unintended ways.
CERT: A Computer Emergency Response Team (CERT) is an organisation formed to study internet security vulnerabilities, and to provide assistance to online sites that become victims of attacks. National CERTS are now in place in most member states, offering a 24-hour emergency response service, information sharing to improve cybersecurity, and also coordinating responses to cybersecurity threats and incidents.
Cloud computing: Cloud computing refers to a computing system in which large groups of remote servers are networked to allow centralised data storage and remote online access to computer services or resources.
Critical infrastructure: Assets that are necessary for the efficient and safe functioning of society, including: computers, systems and networks.
Cybercrime: Cybercrime refers to criminal acts associated with computers, networks, ICT and online activity. Cybercriminals use the internet to commit crimes such as fraud, phishing, and identity theft.
Cyberdefence: Methods used to protect critical infrastructure and/or counter targeted attacks.

Cyber espionage: The stealing of secrets from individuals, groups, competitors, corporations and government entities using information stored in digital formats, on computers, the cloud, and IT networks.
Cybersecurity: Methods used by people, processes and technologies, to prevent, detect and recover from damage to confidentiality, integrity and availability of information in cyberspace. Cybersecurity seeks to protect critical infrastructure.
Cybersecurity strategy: A cybersecurity strategy is a strategic framework that aims to improve the security and resilience of national infrastructure. The document specifies the scope, determines priorities and defines the principles and objectives of cybersecurity on a national level.
Data breach: A data breach is a security incident that occurs when sensitive or confidential data is viewed, copied, stolen or otherwise made available to unauthorised persons.
Denial of Service (DoS): A DoS attack is an attack that shuts down a system. Hackers cause DoS attacks by destroying or manipulating data or by overloading a server with requests so as to prevent it from functioning. DoS attacks are carried out by a person or system.
Distributed Denial of Service (DDoS): A DDoS attack is a form of a DoS attack that shuts down a system and is carried out by multiple computers.
Drive-by download: Programs that a user unwittingly downloads, or downloads without understanding the consequences of such actions. Attackers exploit vulnerabilities in users' browser, emails and applications, or take over control of websites and associated software, e.g. e-payment mechanisms.
Encryption: The process of securing data by ciphering information in a way that even if intercepted it is unreadable unless using the right decoding key (decrypting the message).
Hacker: A hacker is a person who seeks out a weakness in a computer or system and exploits this to gain access to data.
Hactivism: Hactivism is the use of computers and/or networks to promote a social or political message.
Hole: A hole is a vulnerability in the system design that allows attackers to circumvent security measures.
Honeypot: A honeypot is a trap set to detect and deflect the unauthorised use of information systems. It generally consists of a computer, data or a network site that gives the appearance of being part of a network, but that in reality is isolated and monitored.
Information and Communication Technologies (ICT): Technologies through which information is created, distributed, analysed and stored.
Information Society: The Information Society is a society where the creation, use and distribution of information is carried out by computers and networks. It is transformative in all areas of economic, social and political life.
Internet of Things: Technologies that can communicate with each other without requiring human-human or human-computer direction, e.g. with the transfer of data, wireless technologies.

Keylogger: Keyloggers are malicious programs that record the key strokes made by a user, in order to get access to confidential information including usernames and passwords.
Malware: Malware is a generic term used to describe malicious software (code or program) used in a cyberattack, e.g. viruses, Trojan horses, spyware, worms, and other types of malicious agents.
National Cyber Security Centre (NCSC): A national cybersecurity centre is commonly tasked with protecting the national critical infrastructure. The NCSC may coordinate the national security strategy and house the Computer Emergency Response Team (CERT).
Password sniffing: Password sniffing refers to a program that attempts to capture passwords as they cross a network.
Payload: Payload refers to the results produced by a virus attack.
Personal data: Any information relating to an identified or identifiable person.
Pharming: Pharming allows a hacker to redirect internet users to a 'spoofed website' that mimics a legitimate site. The hacker then uses the spoofed site to steal personal information such as usernames, passwords and account information.
Phishing: Phishing is a social engineering technique that attempts to fraudulently acquire users' sensitive data, e.g. personal information, passwords, credit card information, email contacts. It is primarily carried out via email or instant messaging.
Public–Private Partnership (PPP): A PPP is a relationship between the public and private sector, usually as defined in a memorandum of cooperation or outlined in an agreement, which establishes, and sets out to achieve, common goals and objectives.
Ransomware: Ransomware is a growing phenomenon where the attacker installs malicious software that encrypts a user's data. The data is held ransom until a fee is paid.
Rogueware: This is a form of ransomware, in which the attacker tricks the user into paying for the (simulated) removal of malware on their computer
Scareware: Scareware is a type of malware that convinces users that a virus has infected their computer. It then suggests they pay for and download software to remove the fictitious virus.
Social engineering: Social engineering is a technique used by hackers to gain access to a victim's sensitive information or to trick them into installing malicious software. This is often achieved by pretending to be a person or entity familiar to the victim, e.g. a friend, colleague, bank.
Spam: Spam refers to unwanted or unsolicited bulk electronic messages, typically sent to numerous recipients. Spam can include legitimate advertisements, advertisements for illegal products such as pharmaceuticals, phishing emails and emails with malware attached.
Spyware: A type of malware that exploits infected computers by collecting data, e.g. victim's passwords, financial information, search history or route HTTP requests to specific sites. One such application is a keylogger that collects passwords.
Targeted attack: An attack that specifically targets a person, organisation or network.

Tor: Tor is an open source tool that allows anonymous use of the internet by relaying traffic though the computers of other Tor users.
Trojan horse: A Trojan horse is a type of malware that pretends to have a legitimate use or be a benign application but possesses other sinister functions. Unlike viruses, Trojans do not replicate.
Virus: A virus is a type of malware that infects systems by attaching itself to disks or other files and replicating itself repeatedly. The virus can spread when an infected file or application is opened or modified.
Vulnerability: A flaw that exposes the defective software or operating system (OS) to attacks and abuse by hackers who exploit it in order to gain unauthorised access to sensitive information and control over a computer system or a network.
Watering hole: A watering hole is a technique used to attack a target group, e.g. by spotting a weakness or a 'hole' in a popular application, such as Java, and injecting exploit (i.e. a software tool designed to take advantage of a flaw in a computer system) into the application. The user's system will then become infected with the malware.
Worm: Worms are a type of malware that replicate programs but, unlike viruses, do not infect other computer program files. Worms can spread by creating copies on the same computer, or spread to others via a network.
Zero-day attack: A zero-day attack exploits a previously unknown vulnerability in a computer application or operating system, one that has not yet been addressed or patched.
Zombie: A zombie is a PC that is infected with a virus or Trojan horse that puts it under the remote control of a hacker. The hacker uses it to perform malicious tasks such as spamming or launching Denial of Service (DoS) attacks.

TABLE 1. EU FUNDS AND PROGRAMMES RELATED TO CYBER CAPACITY BUILDING

Instruments and funds that currently provide funding for cyber capacity-building projects are marked with *
Instruments and funds that provided funding for cyber capacity-building projects in the past are marked with **

Instrument/Fund	Budget for 2014 - 2020	Geographical scope
***Instrument contributing to Stability and Peace (IcSP)[1]**		
The objective of the IcSP is to address global and trans-regional threats to peace, international security and stability. The EU provides technical and financial assistance in the following areas: threats to law and order, to the security and safety of individuals, to critical infrastructure and to public health. Assistance in those areas includes support for measures aimed at: strengthening the capacity of law enforcement and judicial and civil authorities involved in the fight against organised crime, including cybercrime; addressing threats to critical infrastructure, energy operations and energy distribution, and electronic information and communication networks.	€2.3 billion; out of which €10.5 million for cybercrime and 11 million for cybersecurity for the period 2014-2017	Worldwide
Partnership Instrument (PI)[2]		
The PI is designed to address global challenges such as climate change and energy security and to support the external dimension of EU policies (e.g. competiveness, research and innovation). The external projection of the Europe 2020 Strategy is a major strategic component of the PI, including the focus on promoting policy dialogue in areas of mutual interest to the EU and its partners such as transport, support to growth policies for innovative markets and corporate social responsibility, information and communication technologies, consumer safety, disaster management, regional development and regional integration.	€960.4 million	The EU's strategic partners (BRICS), Asia-Pacific, the Americas, Russia, Central Asia and the Gulf, key international and regional groupings
****The Instrument for Pre-accession Assistance (IPA II)[3]**		
The IPA is the means by which the EU supports reforms in the enlargement countries with financial and technical aid. This support is aimed at helping partners undertaking political and economic reforms, and preparing them for the rights and obligations that come with EU membership. IPA II targets reforms within the framework of pre-defined sectors. These sectors cover areas closely linked to the enlargement strategy, such as democracy and governance, rule of law or growth and competitiveness.	€11.7 billion	Albania, Bosnia and Herzegovina, FYROM, Iceland, Kosovo, Montenegro, Serbia, Turkey.
European Development Fund (EDF)[4]		
The EDF is the EU's main instrument for providing development aid to African, Caribbean and Pacific (ACP) countries and to overseas countries and territories (OCTs). The EDF funds cooperation activities in the fields of economic development, social and human development as well as regional cooperation and integration.	€30.5 billion	ACP countries
Development Cooperation Instrument (DCI)[5]		
The DCI is organised in geographic and thematic programmes. Geographic programmes support cooperation within the following areas: poverty eradication and developing infrastructure and the increased use of information and communication technologies. Thematic programmes benefit all developing countries (including those covered by the ENPI and the EDF). The GPGC programme, in particular, seeks to foster economically, socially and environmentally sustainable development in an integrated and holistic way, taking into account the need to link programming objectives with the aims of promoting good governance, political stability and security.	€19.6 billion out of which €5.1 million for the GPGC programme.	Asia, South Africa, Middle East and Latin America

[1] https://ec.europa.eu/europeaid/sites/devco/files/icsp-strategy-paper-mip-20140812_en.pdf
[2] http://ec.europa.eu/dgs/fpi/documents/pi_mip_annex_en.pdf
[3] http://ec.europa.eu/enlargement/instruments/overview/index_en.htm
[4] http://ec.europa.eu/europeaid/node/1079
[5] https://ec.europa.eu/europeaid/sites/devco/files/mip-gpgc-2014-2017-annex_en.pdf

****European Neighbourhood Instrument (ENI)**[6]		
The ENI contributes to strengthening bilateral relations with partner countries and bringing tangible benefits both to the EU and its partners in areas such as democracy and human rights, the rule of law or sustainable development. The European Neighbourhood-wide measures, in particular, are implemented across all countries of the Neighbourhood, and aim to support partner countries' reform efforts, as well as respond to these countries' needs on the basis of their level of development. The strategic priorities include building a partnership for inclusive economic development and integration and targeted capacity building (i.e. supporting the approximation of the regulatory framework to EU norms and standards).	€15.4 billion out of which €3.1 billion for neighbourhood-wide measures	ENP countries
European Instrument for Democracy and Human Rights (EIDHR)[7]		
The EIDHR is the expression of the EU's intention to integrate the promotion of democracy and human rights into all of its external policies.	€1.3 billion	Civil society organisations
***Internal Security Fund (ISF)**[8]		
The Fund promotes the implementation of the Internal Security Strategy and law enforcement cooperation, among other issues. The ISF Police component contributes to ensuring a high level of security in the EU. The Fund's activities focus on two objectives: combating crime and managing risk and crisis. Funding will be provided for transnational actions identified through a targeted call for proposals aiming at fostering public-private partnerships to fight cybercrime with transnational impact, providing support to an integrated EU approach to prevent and fight cybercrime by enhancing the capabilities of law enforcement authorities and other actors and lending support to projects to prevent and fight child sexual abuse online. Funding will be also used for conducting a third Eurobarometer on cybercrime.	€3.8 billion out of which €1 billion for the ISF Police and €5 million for cybercrime projects more specifically	International organisations or third countries whenever international partnership is necessary for the attainment of the project objectives
***Horizon 2020 Framework Programme for Research and Innovation (H2020)**[9]		
H2020 is the EU's flagship research programme. The 2014/2015 Work Programme focuses on protecting citizens, society and the economy as well as EU assets, infrastructures and services. The funding in the coming years will target: forensics; the ethical/societal dimension (i.e. investigating the role of the social, psychological and economic aspects of the processes that lead to organised crime); the role of ICT in Critical Infrastructure Protection; information-driven cybersecurity management; trust eServices; and value-sensitive technological innovation in cybersecurity.	€97.2 million for Digital Security (Cybersecurity, Privacy and Trust) and €12-17 million for cyber-related forensics	Funding for third countries is however still subject to the Evaluations although in some projects under H2020 the funding is available for Associate and Partner countries
Competitiveness of Enterprises and SMEs Programme – COSME[10]		
COSME – the Programme for the Competitiveness of Enterprises and Small and Medium-sized Enterprises (SMEs) – is an EU programme to strengthen the competitiveness and sustainability of the Union's enterprises and to encourage an entrepreneurial culture and promote the creation and growth of SMEs. COSME projects will seek to explore synergies with other programmes, in particular with regard to developing ICT products and services, e-commerce, e-skills, investment in innovation and research, technology transfer, networking, clusters and Key Enabling Technologies.	€2.3 billion	Montenegro, FYROM, Serbia (2015), Turkey, Albania (2014) Moldova, Iceland. Other interested countries might receive funding after joining COSME.

[6] http://eeas.europa.eu/enp/pdf/financing-the-enp/enp_wide_strategic_priorities_2014_2020_and_multi_annual_indicative_programme_2014_2017_en.pdf
[7] http://ec.europa.eu/europeaid/sectors/human-rights-and-governance/democracy-and-human-rights/partners-and-actors_en
[8] http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/index_en.htm
[9] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-security_en.pdf
[10] http://ec.europa.eu/enterprise/initiatives/cosme/index_en.htm

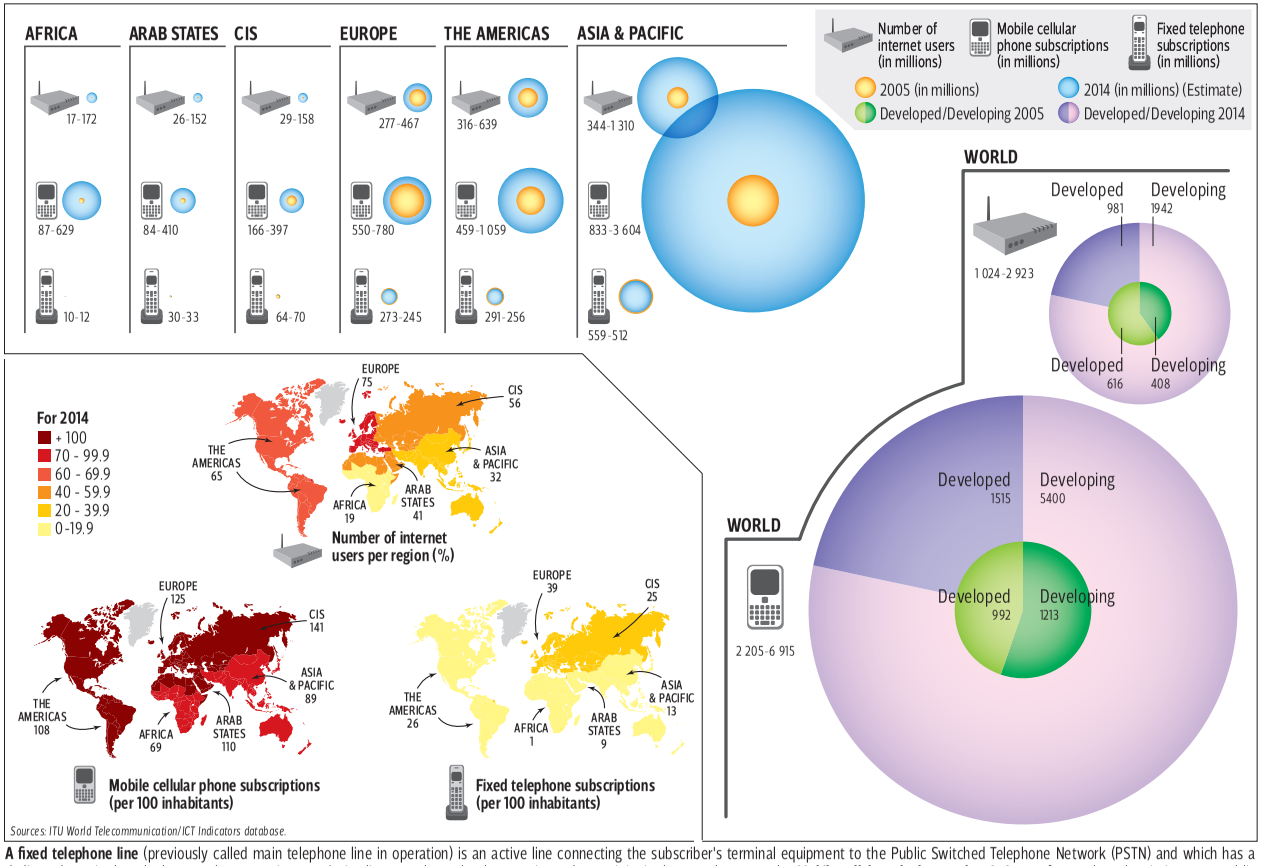
TABLE 2. CAPACITY-BUILDING PROJECTS IMPLEMENTED BY THE EU OR WITH THE SUPPORT OF EU FUNDS

Project	Objectives	Budget and a source of funding	Implementing partner	Beneficiaries
COMPLETED				
Project on cybercrime in Georgia	To help Georgia develop a consistent policy to combat cybercrime in view of implementing the Convention on Cybercrime (CETS 185)	€220,000 The project is funded by the European Union with co-funding from the CoE	Council of Europe	Georgia
Cybercrime@IPA	To strengthen the capacities of criminal justice authorities in the relevant areas to cooperate effectively against cybercrime based on the Budapest Convention on Cybercrime and other standards	€2.78 million European Union (IPA Regional Programme 2010) and CoE	Council of Europe	Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, FYROM, Turkey, Kosovo
CyberCrime@EAP	To strengthen the capacities of Eastern Partnership countries to cooperate effectively against cybercrime	€894,000 European Union (ENPI)	Council of Europe	Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine.
ACP-Information and Communication Technologies (@CP-ICT)	To help ACP governments and institutions to design, implement, monitor and evaluate their national, regional and continental ICT policies towards sustainable development	€20 million 9th European Development Fund	ACP Secretariat	African, Caribbean and Pacific Group of States
ONGOING				
The Global Action against Cybercrime (GLACY)	Promoting accession to the Budapest Convention on Cybercrime and enabling criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of this treaty. The GLACY Project is conceived as a resource to support, in a pragmatic manner, states that are prepared to implement the Budapest Convention on Cybercrime.	€3.35 million European Union (IcSP) and CoE	Council of Europe, with the European Cybercrime Centre, the French Ministry of Interior and the Romanian Ministries of Justice and of Interior as project partners.	Global scope

Enhancing Cyber Security	To increase the security and resilience of Information Communication Technologies networks in the beneficiary countries by building and training local capacities to adequately prevent, respond to and address cyberattacks and/or accidental failures and by establishing an appropriate legal framework where applicable.	€1.5 million European Union (IcSP)	Consortium led by ADETEF (France) in partnership with CIVIPOL Conseil.	FYROM, Kosovo, Moldova
PLANNED				
Capacity Building for Cybercrime	Supporting the adoption and implementation of cybercrime and cybersecurity strategies; and also strengthening the capacity of law enforcement and criminal justice authorities to effectively investigate, prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.	€9.5 million European Union (IcSP)	Council of Europe and Interpol, in cooperation with the European Cybercrime Centre and interested member states	Africa and Asia
Protecting Critical Infrastructure	To build capacities in third countries to adequately prevent, respond to and address cyberattacks and/or accidental failures	€11 million European Union (IcSP)	TBD	TBD
Fighting cybercrime and child sexual abuse	To create Public-Private Partnerships (PPPs) to fight cybercrime; to support an integrated EU approach to prevent and fight cybercrime by strengthening the capabilities of law enforcement authorities; and to prevent and fight against child sexual abuse online, including the 'Global Alliance against Child Sexual Abuse Online'	€5 million European Union (ISF-P)	TBD	TBD

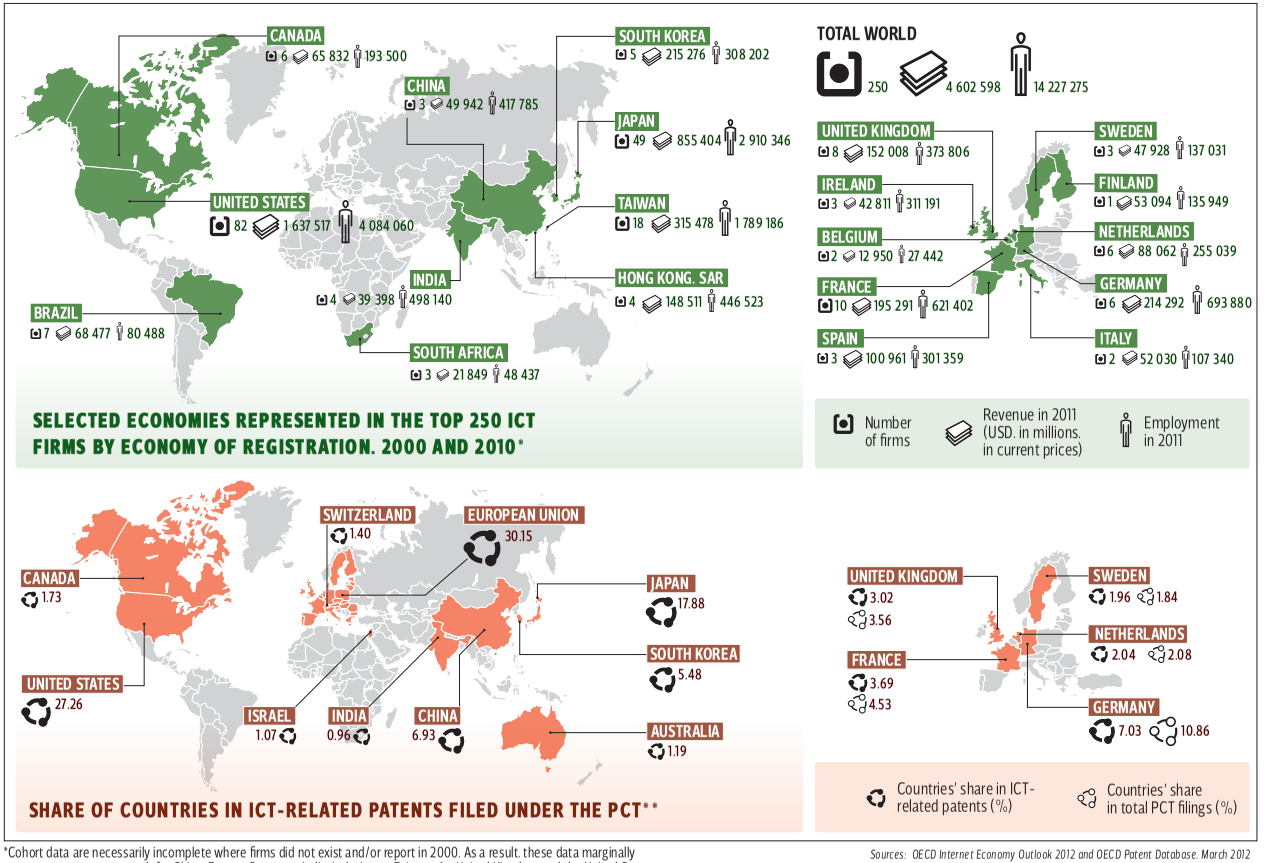
MAPS AND CHARTS

1- GLOBAL EVOLUTION IN NUMBER OF INTERNET USERS, MOBILE AND FIXED LINE SUBSCRIPTIONS



A fixed telephone line (previously called main telephone line in operation) is an active line connecting the subscriber's terminal equipment to the Public Switched Telephone Network (PSTN) and which has a dedicated port in the telephone exchange equipment. Active lines are those that have registered an activity in the past three months. **Mobile cellular telephone subscriptions** refers to the subscriptions to a public mobile telephone service that provides access to a Public Switched Telephone Network (PSTN) using cellular technology, including the number of pre-paid SIM cards active during the past three months. This includes both analogue and digital cellular systems (3G and 4G) subscriptions, but excludes mobile broadband subscriptions via data cards or USB modems. **Number of internet users** refers to the estimated number of internet users out of the total population. This includes those using the internet from any device (including mobile phones) in the last 12 months.

2 - GLOBAL DISTRIBUTION OF TOP ICT COMPANIES AND ICT-RELATED PATENTS

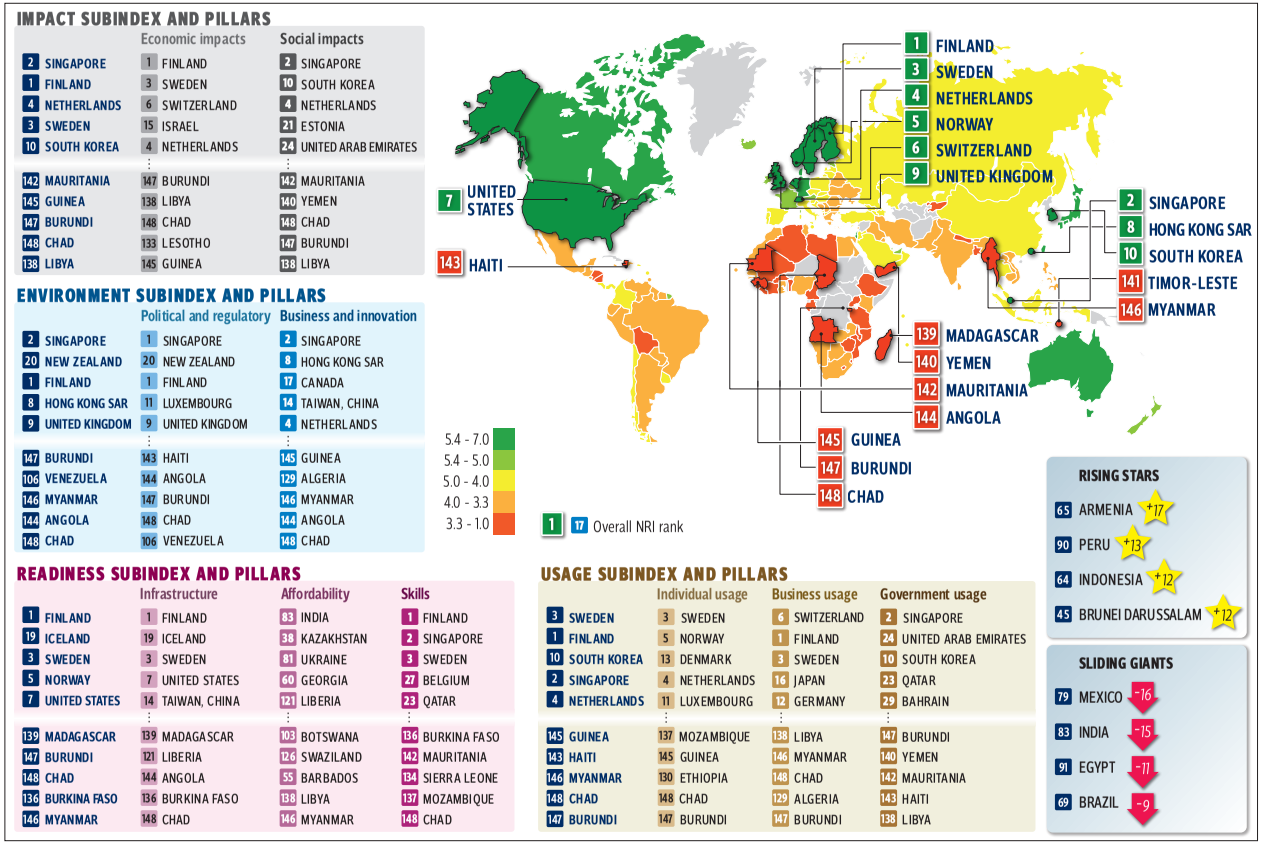


*Cohort data are necessarily incomplete where firms did not exist and/or report in 2000. As a result, these data marginally exaggerate revenue growth for China, France, Germany, India, Italy, Japan, Taiwan, the United Kingdom and the United States.

** Patent applications filed under the Patent Co-operation Treaty, at international phase, designating the European Patent Office.

Sources: OECD Internet Economy Outlook 2012 and OECD Patent Database, March 2012

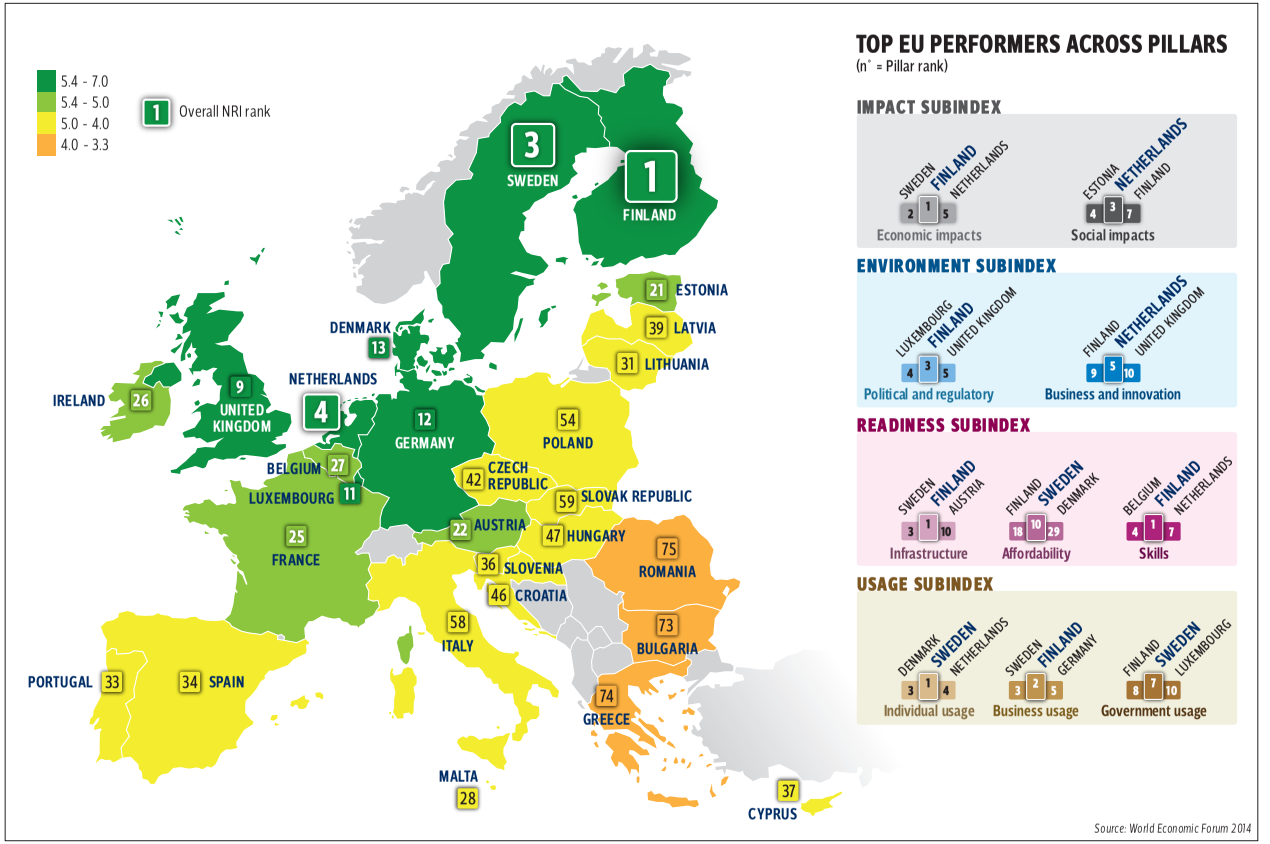
3 - NETWORK READINESS INDEX 2014: BEST AND WORST PERFORMERS



Note: The Networked Readiness Index measures, on a scale from 1 (worst) to 7 (best), the performance of 148 economies in leveraging information and communication technologies to boost competitiveness and well-being.

Source: World Economic Forum 2014

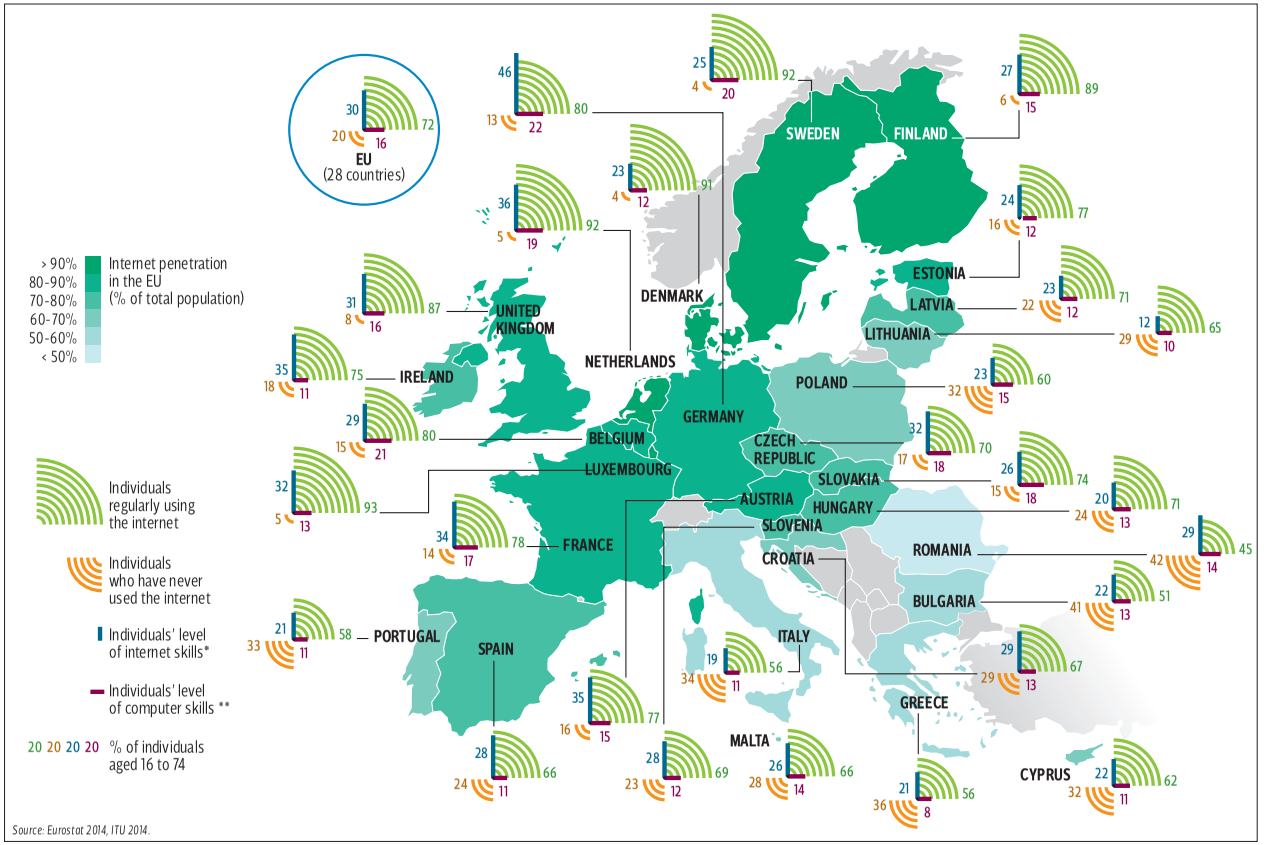
4 - EU COUNTRIES IN THE NETWORK READINESS INDEX 2014



Source: World Economic Forum 2014

The environment subindex gauges the friendliness of a country's market and regulatory framework in supporting high levels of ICT uptake and the emergence of entrepreneurship and innovation-prone conditions. **The readiness subindex** measures the degree to which a society is prepared to make good use of an affordable ICT infrastructure and digital content. **The usage subindex** assesses the individual efforts of individuals, business and government to increase their capacity to use ICT as well as their actual use in their day-to-day activities with other agents. **The impact subindex** measures the broad economic and social impacts of ICT on competitiveness and well-being, reflecting the transformation towards an ICT- and technology-savvy economy and society.

5 - USE OF INTERNET AND COMPUTER/INTERNET SKILLS IN THE EU

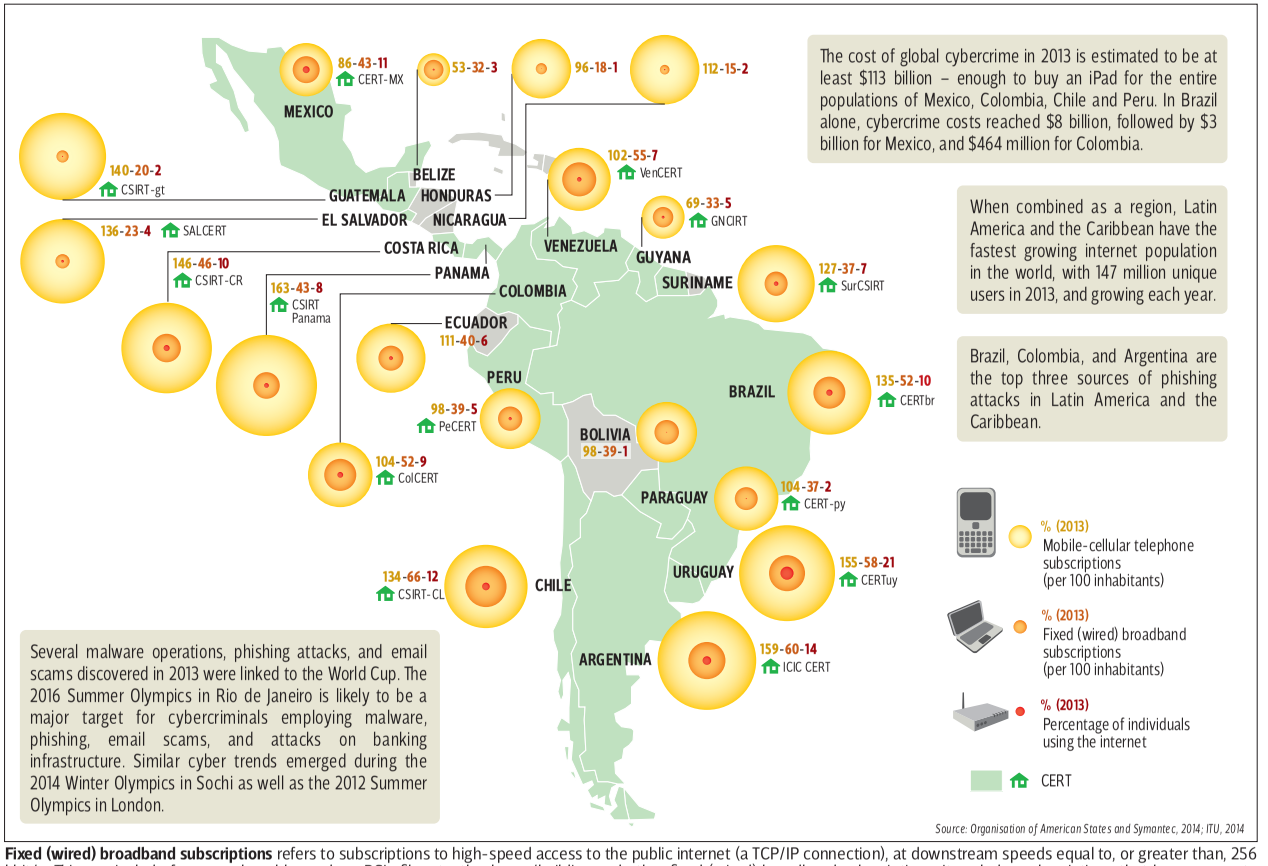


Source: Eurostat 2014, ITU 2014.

* The percentage of individuals who have carried out 1 or 2 of the 6 following internet-related activities: use a search engine to find information; send an e-mail with attached files; post messages to chatrooms, newsgroups or any online discussion forum; use the internet to make telephone calls; use peer-to-peer file sharing for exchanging movies, music etc.; create a web page. Data from 2013.

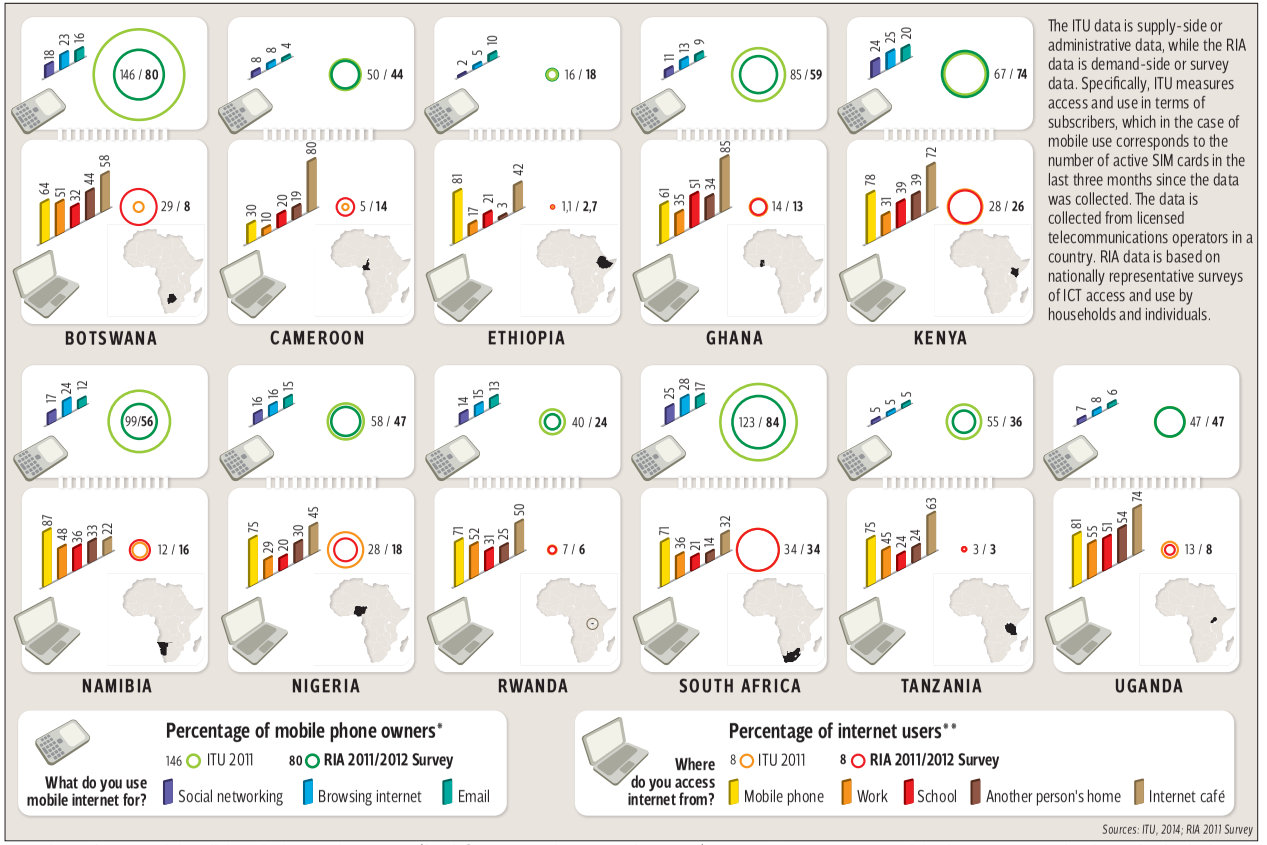
**The percentage of individuals who have carried out 1 or 2 of the 6 following computer-related activities: copy or move a file or folder; use copy and paste tools to duplicate or move information within a document; use basis arithmetic formula (add, substract, multiply, divide) in a spreadsheet; compress files; connect and install new devices, e.g. a printer or a modem; write a computer program using a specialised programming language. Data from 2012.

6 - DEVELOPMENT OF ICT INFRASTRUCTURE IN LATIN AMERICA



Fixed (wired) broadband subscriptions refers to subscriptions to high-speed access to the public internet (a TCP/IP connection), at downstream speeds equal to, or greater than, 256 kbit/s. This can include for example cable modem, DSL, fibre-to-the-home/building and other fixed (wired) broadband subscriptions. It excludes subscriptions that have access to data communications (including the internet) via mobile cellular networks.
Mobile cellular telephone subscriptions refers to the subscriptions to a public mobile telephone service that provides access to a Public Switched Telephone Network (PSTN) using cellular technology, including the number of pre-paid SIM cards active during the past three months. This includes both analogue and digital cellular systems (3G and 4G) subscriptions, but excludes mobile broadband subscriptions via data cards or USB modems.
Number of internet users is the estimated number of internet users out of the total population. This includes those using the internet from any device (including mobile phones) in the last 12 months.

7- COUNTING THE ICT USERS IN AFRICA: DIFFERENT METHODS, DIFFERENT OUTCOMES

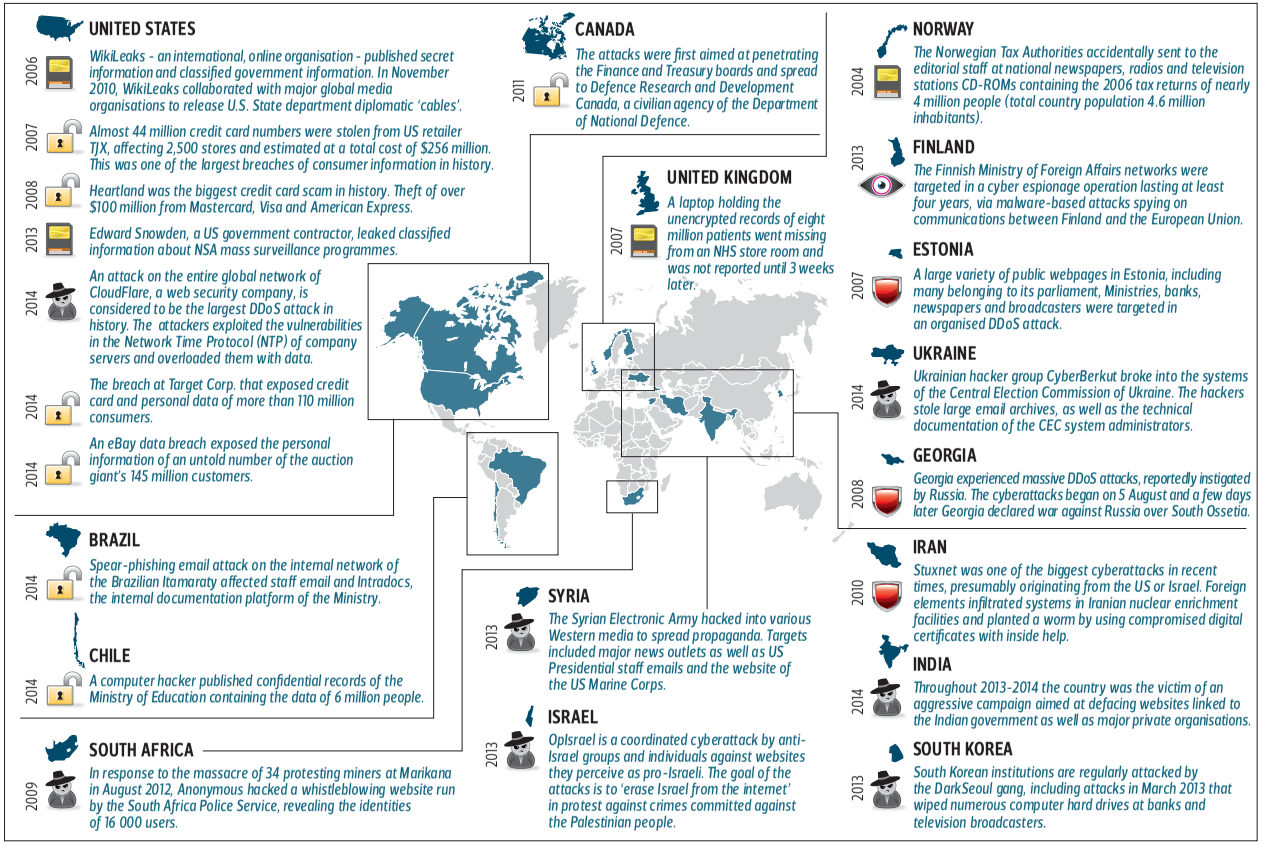


The ITU data is supply-side or administrative data, while the RIA data is demand-side or survey data. Specifically, ITU measures access and use in terms of subscribers, which in the case of mobile use corresponds to the number of active SIM cards in the last three months since the data was collected. The data is collected from licensed telecommunications operators in a country. RIA data is based on nationally representative surveys of ICT access and use by households and individuals.

* ITU data refers to mobile cellular telephone subscriptions (for definition, see the note under map 6). RIA 2011/2012 measures mobile phone access as the share of individuals aged 15 years or older who own a mobile phone in the total population. The number includes mobile phones with and without internet access. The data about the use of mobile internet is based on RIA 2011/2012.

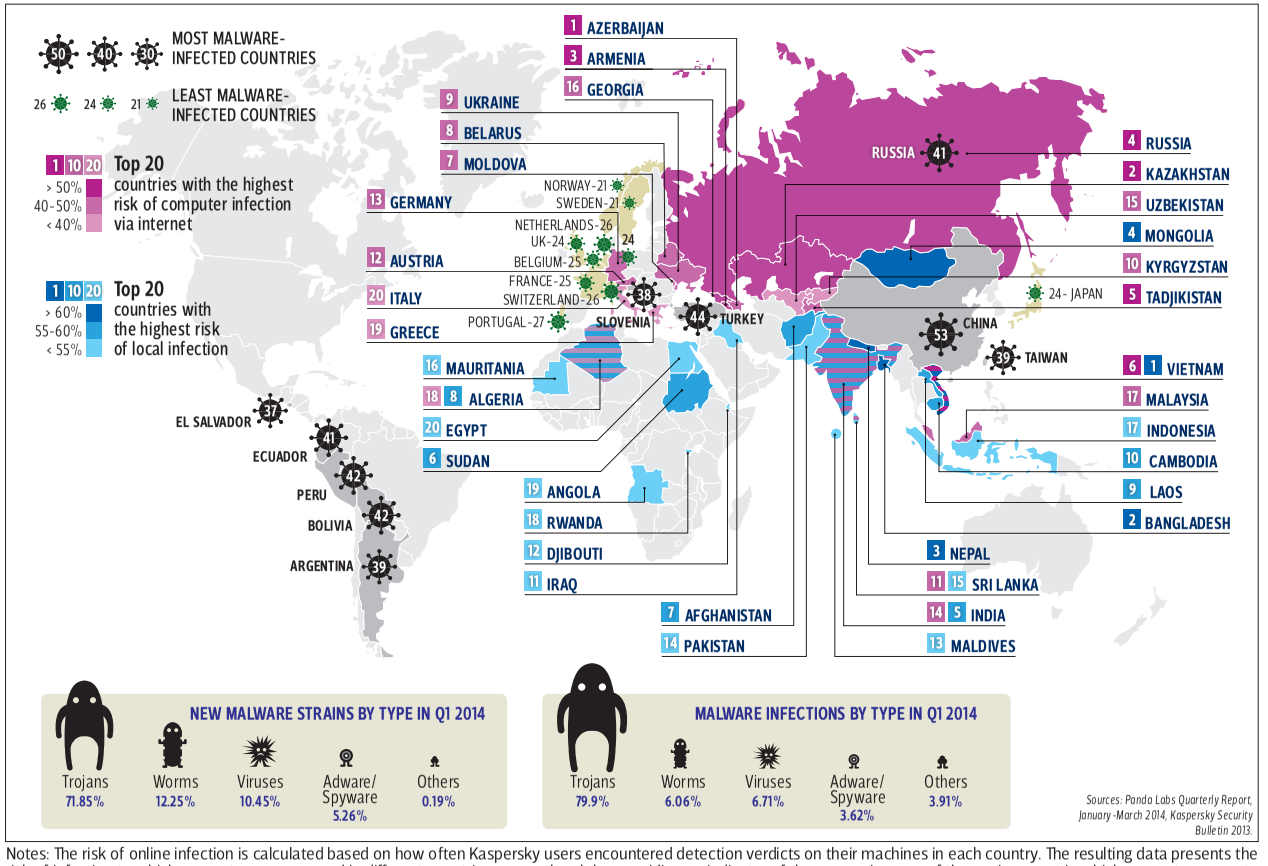
**ITU data refers to the number of internet users indicator (for definition, see the note under map 6). RIA 2011/2012 measures internet users defined as individuals aged 15 years or older who have used the internet. The data about the access to internet is based on RIA 2011/2012 and covers the last 12 months from when the question was asked.

8 - EXAMPLES OF MAJOR CYBER INCIDENTS WORLDWIDE



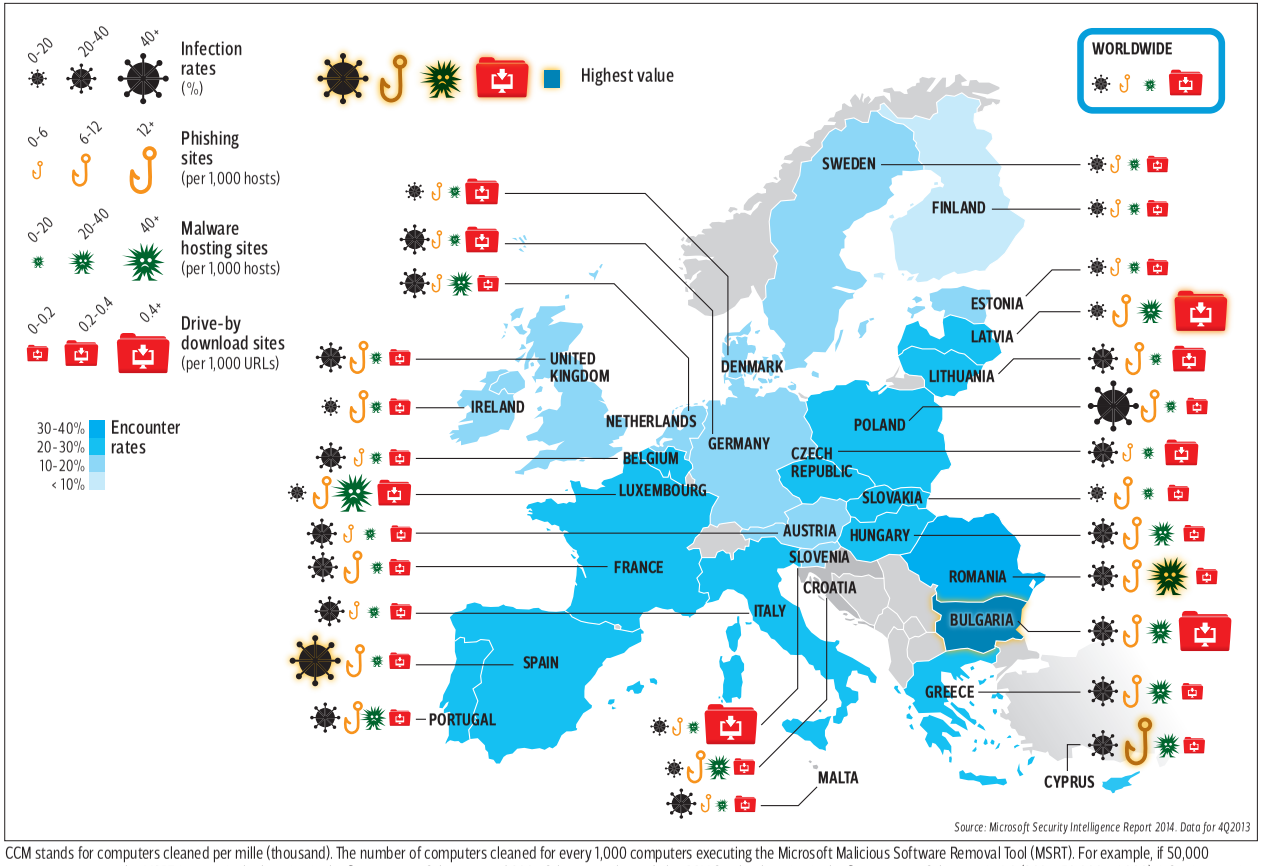
Sources: Kaspersky Security Bulletin 2013; Information is Beautiful Database, ZDNet.

9 - GLOBAL DISTRIBUTION OF MALWARE AND RISK OF INFECTION



Notes: The risk of online infection is calculated based on how often Kaspersky users encountered detection verdicts on their machines in each country. The resulting data presents the risk of infection to which computers are exposed in different countries across the globe, providing an indicator of the aggressiveness of the environment in which computers operate in different countries. The risk of local infection rate is measured by scanning the hard drive and the removable devices of Kaspersky products users. The computers were infected by other means than via the internet, network ports and mail (in other words, excluding infections via the internet).

10 - SELECTED CYBER THREATS IN THE EU



CCM stands for computers cleaned per mille (thousand). The number of computers cleaned for every 1,000 computers executing the Microsoft Malicious Software Removal Tool (MSRT). For example, if 50,000 computers execute the MSRT in a particular location in the first quarter of the year and 200 of them are cleaned, the CCM for that location in the first quarter of the year is 4.0 (200 ÷ 50,000 × 1,000). Infection rate is the percentage of computers running Microsoft real-time security software that report detecting malware, or report detecting a specific threat or family, during a period.

ABBREVIATIONS

ANSAC	ASEAN Network Security Action Council
ANSSI	*Agence nationale de la sécurité des systèmes d'information* (French national agency for the security of Information Systems)
ART	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
AU	African Union
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CICTE	Inter-American Committee against Terrorism
CIIP	Critical Information Infrastructure Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COMESA	Common Market for Eastern and Southern Africa
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CSOC	Cyber Security Operations Centre
CTO	Chief Technology Officer
DAC	Development Assistance Committee
EAC	East African Community
ECCAS	Economic Community of Central African States
ECOWAS	Economic Community of West African States
ENP	European Neighbourhood Policy
GPGC	Global Public Goods and Challenges
IAEA	International Atomic Energy Agency
IcSP	Instrument contributing to Stability and Peace
ICT	Information and Communication Technologies
IGAD	Intergovernmental Authority on Development
OAS	Organisation of American States
OCSIA	Office of Cyber Security and Information Assurance
ODA	Official Development Assistance
OECD	Organisation for Economic Cooperation and Development
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
R&D	Research and Development
RFID	Radio-Frequency Identification
SADC	Southern Africa Development Community
UNDP	United Nations Development Programme
WEF	World Economic Forum

NOTES ON THE CONTRIBUTORS

Enrico Calandro is a Research Fellow at Research ICT Africa and a doctoral candidate in Managing Infrastructure Reform and Regulation at the Graduate School of Business, University of Cape Town. Prior to that, he worked as a technical advisor for the ICT programme of the SADC Parliamentary Forum in Namibia, within the UN technical cooperation framework. He is a recipient of the Amy Mahan Ph.D scholarship award for the advancement of ICT policy and regulatory research in Africa, of the UNDESA fellowship for international cooperation and of the Emerald Literati Network Award for Excellence 2013 and 2014. His academic research focuses on internet governance and on ICT access and use in Africa.

Elena Kvochko is Manager for the IT Industry and the Partnership for Cyber Resilience project at the World Economic Forum. She manages the global partnership programmes on cybersecurity and the Internet of Things and is responsible for building relationships with top information technology industry players. The World Economic Forum (WEF) provides a platform for CEOs, business executives, and policy leaders to convene and define the industry agenda at the global and regional levels. Prior to the Forum, Elena worked as Information and Communication Technology specialist at the World Bank and focused on a portfolio of projects to leverage ICT for economic growth, job creation and effective governance in emerging economies.

Patryk Pawlak is a Senior Analyst at the European Union Institute for Security Studies (EUISS) where he currently leads the EUISS Cyber Task Force. Before joining the Institute, he worked with numerous research institutions, including the Center for Transatlantic Relations at Johns Hopkins University, the Center for Peace and Security Studies at Georgetown University and the Centre for European Policy Studies in Brussels. He was also a fellow in the European Foreign Policy Studies Programme and the Transatlantic Post-Doc Fellowship for International Relations and Security (TAPIR). His current research interests include cyber capacity building and the ethical aspects of security and surveillance technologies. He holds a Ph.D in Political Science from the European University Institute in Florence.

Maria Grazia Porcedda is Research Associate with the SURVEILLE project. She previously worked at the Centre de Recherche Informatique et Droit (CRID, FUNDP) on privacy and cloud computing, and as a trainee on privacy issues at both the Organisation for Economic Co-operation and Development (DECD) and the European Data Protection Supervisor. She holds an LL.M in Comparative European and International Law from the European University Institute in Florence and an MA in International Relations from the University of Bologna. She is currently completing

her Ph.D thesis at the EUI on the reconciliation of privacy and data protection with the prevention of cybercrime and the pursuit of cybersecurity.

Neil Robinson is a Research Leader at RAND Europe, working on such areas as European cybersecurity policy, cyber defence capabilities, and the broader socioeconomic implications of the Information Society. He has coordinated numerous studies for EU institutions – including the European Defence Agency and the European Commission – and advised several national agencies, including the UK Office of Cyber Security and Information Assurance (OCSIA) and Defence Science and Technology Laboratory, the French Interagency Joint Doctrine Centre (CICDE), and the Swedish Centre for Asymmetric Threat Studies (CATS). He received his BA in War Studies and History from King's College London and his M.Sc. in Information Systems and Technology from City University London.

BIBLIOGRAPHY

- Andrianaivo, Mihasonirina and Kpodar, Kangni. 'ICT, Financial Inclusion, and Growth: Evidence from African Countries', *IMF Working Paper WP/11/73,* 2011.
- Austrian Development Agency, *Manual Capacity Development: Guidelines for implementing strategic approaches and methods in ADC*, August 2011.
- Bilbao-Osorio, Beñat, Dutta, Soumitra and Lanvin, Bruno (eds.). *The Global Information Technology Report 2014: Rewards and Risks of Big Data*, World Economic Forum, Geneva, 2014.
- Burt, David, Kleiner, Aaron, Nicholas, Paul and Sullivan, Kevin. 'Cyberspace 2025: Navigating the future of cybersecurity policy', Microsoft Corporation, June 2014.
- Burt, David, Nicholas, Paul, Sullivan, Kevin and Scoles, Travis. 'The Cybersecurity Risk Paradox: Impact of Social, Economic, and Technological Factors on Rates of Malware', *Microsoft Security Intelligence Report Special Edition (SIR)*, Microsoft Corporation, January 2014.
- Calandro, Enrico, Gillwald, Alison and Zingales, Nicolo. 'Mapping Multistakeholderism in Internet Governance: Implications for Africa', *Evidence for ICT Policy Action – Discussion Paper*, Research ICT Africa, Cape Town, 2013.
- Center for Strategic and International Studies and McAfee. *Net Losses: Estimating the Global Cost of Cybercrime – Economic impact of cybercrime II*, June 2014.
- CISCO and Global Business Network. *The Evolving Internet: Driving Forces, Uncertainties, and Four Scenarios to 2025*, CISCO 2010.
- Council of Europe. *Capacity Building on Cybercrime – Discussion Paper*, 1 November 2013.
- Council of the European Union. *Council conclusions on the Commission 2013 report on the application of the EU Charter of Fundamental Rights and the consistency between internal and external aspects of human rights' protection and promotion in the European Union*, Luxembourg, 5-6 June 2014.
- Council of the European Union. *Council conclusions on a rights-based approach to development cooperation, encompassing all human rights*, Brussels, 19 May 2014.
- Council of the European Union. *EU Human Rights Guidelines on Freedom of Expression Online and Offline*, Brussels, 12 May 2014.
- Danish International Development Agency. *Using ICT to promote governance*, DANIDA study, April 2012.
- Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). *Capacity works. Success stories. Examples of best practices*. Available at: http://www.giz.de/en/downloads/giz2012-en-capacity-works-sucess-stories.pdf
- Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). *Capacity works: the management model for sustainable development*. Available at: https://www.giz.de/en/downloads/gtz2009-en-capacity-works-manual.pdf

- European Commission. *A stronger role of the private sector in achieving inclusive and sustainable growth in developing countries*, Brussels, 13 May 2014.
- European Commission. Commission staff working document: Tool-Box – 'A rights-based approach, encompassing all human rights for EU development cooperation', Brussels, 30 April 2014.
- European Commission. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7 February 2013.
- Evans, Dave. *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*, CISCO, April 2011.
- EY. 'Overcoming compliance fatigue: Reinforcing the commitment to ethical growth', *Thirteen Global Fraud Survey*, EY, 2014.
- Flynn Goodwin, Cristin and Nicholas, Paul. *Developing a National strategy for Cybersecurity: Foundations for Security, Growth, and Innovation*, Microsoft Corporation, October 2013.
- Fukuda-Parr, Sakiko, Lopes, Carlos and Malik, Khalid (eds.). *Capacity for Development: New Solutions to Old Problems*, Earthscan, London, 2002.
- Griffiths, Jesse, Martin, Matthew, Pereira, Javier and Strawson, Tim (eds.). *Financing for development post-2015: improving the contribution of private finance*, European Parliament, Brussels, 2014.
- Heeks, Richard. 'ICT4D 2016: new priorities for ICT4D. Policy, Practice and WSIS in a post-2015 world', *Development Informatics Working Paper Series*, Paper no. 59, 2014.
- International Atomic Energy Agency. 'Computer security at nuclear facilities', *IAEA Nuclear Security Series*, no. 17, Vienna, 2011.
- International Telecommunications Union. *Tracking four years of achievements: implementing the Hyderabad Action Plan*, ITU, Geneva, 2014.
- International Telecommunications Union. *World Telecommunication/ICT Indicators database 2014*, 18th Edition, June 2014.
- Kim, Yongsoo, Kelly, Tim and Raja, Siddhartha. *Building broadband: strategies and policies for the developing world*, World Bank, January 2010.
- Kaspersky Lab. *Kaspersky Security Bulletin 2013*.
- Kleiner, Aaron, Nicholas, Paul and Sullivan, Kevin. *Linking Cybersecurity Policy and Performance*, Microsoft Corporation, February 2013.
- Libicki, Martin C., Senty, David and Pollak, Julia. 'Hackers wanted. An examination of the cybersecurity labour market', RAND, 2014.
- McKinsey Global Institute. *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*, May 2011.
- Organisation for Economic Cooperation and Development (OECD). *Recommendation of the Council on the management of digital security risk for economic and social prosperity*, Draft version DSTI/ICCP/REG(2014)2, 18 March 2014.
- Organisation for Economic Cooperation and Development (OECD). *Evaluating development activities. Providing evidence on results for learning and decision making*, Paris, 2013.
- Organisation for Economic Cooperation and Development (OECD). 'Cybersecurity Policy Making at a turning Point: Analysing a New Generation of National

Cybersecurity strategies for the Internet Economy', *OECD Digital Economy Papers*, no. 211, 2012.
- Organisation for Economic Cooperation and Development (OECD). 'The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy', *OECD Digital Economy Papers*, no. 209, 2012.
- Organisation of American States and Symantec. *Latin American and Caribbean Cybersecurity Trends*, June 2014.
- Pénicaud, Claire and Katakam, Arunjay. *State of the Industry 2013. Mobile Financial Services for the Unbanked,* GSMA, Mobile Money for the Unbanked, London, 2013.
- Research ICT Africa. *Household and Individual ICT Access and Use in Africa, 2011/2012*, Cape Town, 2012.
- Stork, Christoph, Calandro, Enrico, and Gillwald, Alison. 'Internet going mobile: internet access and use in 11 African countries', Info: *The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*, vol. 15, no. 5, 2013, pp.34 -51.
- Symantec. *Internet Security Threat Report*, vol. 19, April 2014.
- Symantec. *Internet Security Threat Report*, vol. 18, April 2013.
- United Nations Development Programme. *Human Development Report 2014. Sustaining Human Progress: Reducing Vulnerabilities and Building Resilience*, New York, 2014.
- United Nations Development Programme. *ICTs and e-governance in UNDP: 2013 Status Report*, New York, 2013.
- World Bank. *World Development Report 2014. Risk and Opportunity: Managing Risk for Development*, Washington, D.C., October 2013.
- World Bank. *ICT for greater development impact. Information and Communication Technology*, 15 June 2012
- World Economic Forum. *Risk and responsibility in a hyperconnected world – Implications for enterprises*, January 2014.
- World Economic Forum. *Global Risks 2014,* 2014.
- World Economic Forum. *Risk and Responsibility in a Hyperconnected World – Pathways to Global Cyber Resilience*, June 2012.

European Union Institute for Security Studies
100, avenue de Suffren | 75015 Paris | France | www.iss.europa.eu