Norwegian Institute of International Affairs

Policy Brief
[15 / 20115]

Cyber Security Capacity Building in Developing Countries

Lilly Pijnenburg Muller

Summary

Cyberspace is an intrinsic part of the development of any country. A strong cyber capacity is crucial for states to progress and develop in economic, political and social spheres.[1] The need to integrate cyber capacity building and development policies has been documented by both the cyber community, academia and policy makers. The investment in securing cyberspace is crucial, as it affects the success rate of other policy initiatives as well. However, there is a clear need for a deeper dialogue with the development community and recipient countries in order to better understand how to implement cyber capacities in practice in order to achieve broader development goals. To stimulate the debate on cyber capacity building and its on social and economic development worldwide this brief puts forward challenges to implementation. The aim to is to set priorities and identify indicators of success and failure. To steer this process a better overview of initiatives and avoid duplication, it is necessary to set up the challenges that both the donors and recipients face. By doing this we move cyber capacity building one step closer to successful implementation.

Introduction

Cyberspace is growing at a speed unprecedented by any other commodity. Almost three billion people are now connected in cyberspace through the Internet; a figure growing rapidly and estimated to reach five billion people, using 50 billion devices, by 2020. As most of this growth will take place in emerging economies, it is not surprising that the development community is pondering how to leverage the benefits accruing from the use of cyberspace and Information and Communication Technologies (ICT) through cyber-capacity building (CCB).[2] This exercise will however be futile if not backed up by a serious discussion about the need to address the challenges posed by the proliferation of ICT infrastructure and Internet applications for sustainable development.

Cyber capacity building in developing countries

Cyberspace is an intrinsic part of the development of any country. A strong cyber capacity is crucial for states to progress and develop in economic, political and social spheres.[3] The rapid growth of and global access to ICT, combined with economic growth, has resulted in a great many first-time users in developing countries. Indeed, the fastest growth in Internet users today is in developing countries – in Asia and Africa in particular[4] (ITU, 2014). Cyberspace knows

1 Pawlak, P. (ed.), Riding the digital wave: The impact of cyber capacity building on human development, ISSUE, report nr 21.

2 The importance of ICT for development was acknowledged at the World Summits on the Information Society that took place in Geneva (2003) and Tunis (2005). Further, the UN has recognized ICT connectivity as 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. There has come a recognition of the diffusion of new technologies that open new possibilities of empowerment for the poor by providing them with access to services otherwise difficult to access, such as banking and health information.

3 Pawlak, P. (ed.) (2014) Riding the digital wave: The impact of cyber capacity building on human development, ISSUE, report nr 21.

4 Much of the growth has been fuelled by a dramatic increase in the use of mobile technology. See Ericsson (2014) Sub-Saharan Africa: Ericsson mobility report appendix. Available at: [Accessed: 1 April 2015]

no boundaries, meaning that developing countries face many of the same cyber threats as the developed world does. These threats can range from malware to cyber-crime, in the form of attacks on state infrastructure, information technology, vital industry and individuals. As proper network, security and legal framework often lacks in these countries developing countries have fewer capabilities for dealing with these challenges than the developed world does. This makes them vulnerable to cybercrime and increases the chances of being attacked. The scarcity of infrastructure to handle cyber-attacks, combined with increased use of technology is a pressing matter. It can both mean greater risks of malware in the form that hackers can take advantage of the inadequate protection put in place by ill-prepared governments and businesses and an inability to punish those that attack through cyberspace. Increased access can in other words mean more harm than good, if it is not accompanied by the capacity to maintain and enable it. That is why cyber capacity building – in addition to market mechanisms – has become a key instrument available to the donor community for ensuring a minimum level of cybersecurity across the globe.

On paper CCB allows developed nations to share the knowledge they have with, and assist developing nations on cyber capacity – finding the right way to do this in practice is another matter. Cyber capacity building requires a horizontal approach across different development policy fields, focusing on improving governance, protecting infrastructure, endorsing the rule of law and providing training.[5] Support and assistance is provided to developing nations to increase their access to, and ability to fully benefit from, the Internet and other elements of cyberspace. Many organizations, national and international, are grappling with how to build cyber capacity in developing countries. Approaches vary in focus from local, state to regional; from a specific area within CCB to all-encompassing. Some assess all levels of cyber capacity within a state; others map out the differences in each country, while yet others focus on specific aspect of the state, such as building a legal framework or Computer emergency response team (CERT).[6] While the various approaches allow for different ways of analysing CCB, few, if any, address how to implement CCB and the challenges thereto and implementation.

Challenges in cyber capacity building

The challenge is to create a structure and institutional stability as early as possible and to integrate this into the local system when building cyber capacities. This can allow for a maximal utilization of the Internet and secure its users against malware. CCB is not immune to the dilemmas inherent in any type of activity within the donor-recipient relationship. Learning from the capacity-building experience of other sectors is essential. Projects predominantly shaped and implemented by external donors are less likely to prove sustainable than those with a significant internal ownership. The next section will focus on the additional challenges that arise as a result of the complex intrinsic nature of cyberspaces, which complicates capacity building. Developing countries face challenges in all types of activities connected to CCB – from human resources development, institutional reform, organizational adaptions, and in the support provided to increase their access to, and ability to fully benefit from, the Internet and other elements of cyberspace. The challenges in securing cyberspace are found not only in the developing countries, but in the donor countries as well. No country faces the same challenge, and no one size fits all, but one size fits most,[7] and these are crucial to map out. If we know the challenges to CCB, the solutions to the issue at hand, on both sides, can be proposed. By doing so CCB moves one step closer to successful implementation. To simplify, these are divided into challenges for donor and developing countries, although the issues are found on, and are affected by, both sides.

Challenges for developing countries

1. Access versus institutional stability

Access to cyberspace is growing faster than the institutions and frameworks that states use to support it. Structures and institutional stability that allows for a utilization of the Internet, while simultaneously guarding the users against malware threats need to be created. To this end, critical infrastructure must be strengthened and efforts made to include cyberspace in existing legal frameworks. Too often, countries tend to think they need assistance in areas other than what should in fact be prioritized for sustainable cyber capacity. For example, a county may ask for assistance to build a CERT – but without having the capacity, or knowledge, to uphold one.

2. Building knowledge, understanding and awareness

Education about the threats and risks that come with cyberspace is essential in today's world of escalating use of cyberspace through increased access. Inadequate understanding of the importance of cybersecurity and cyber hygiene, as in the steps that computer users can take to improve their cybersecurity and better protect themselves online, is a major threat to CCB. However awareness building is difficult if cybersecurity is not a government priority. A comprehensive understanding within governments is needed of the necessity of securing cyberspace and the technological challenges required. Otherwise, implementation of cybersecurity becomes difficult. The number of stakeholders that need to be engaged, the challenge of being proactive in managing these risks, and the difficulty of conveying an understanding of the overall purpose security measures should serve, complicates the matter and provides additional challenges. Lack of knowledge on how to improve cyber capacity limits the development thereof.

5 ISSEU (2014) Cyber capacity building as a development issue: What role for regional organisations? Conferences, Task forces - 13 March 2014. Available at: http://www.iss.europa.eu/activities/detail/article/cyber-capacity-building-as-a-development-issue-what-role-for-regional-organisations/ [Accessed: 1 April 2015]

6 For an assessment of the work done to date see Muller, L.,P. (2015) Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities (NUPI: Oslo)

7 European Union Institute for Security Studies (ISSEU) (2014) Cyber Capacity Building in Ten Points (ISSEU, Paris)

3. Legal framework
An adequate legislative framework that can enact decisions for building a secure cyberspace is essential. Regional institutions like the AU and EU argue for a legislative framework as the backbone of cybersecurity and emphasized the need for a solid regulatory framework.[8] Including cyberspace in a legislative framework is however a challenge – not least as regards to deciding the size and amount of regulations to include and how broad a framework to aim at. A legal framework that reaches too broadly and is too ambitious is difficult to uphold; however, a framework that does not include enough is no solution either. The challenge is thus to strike a balance between these two.

4. Affordability
Many countries lack resources to build what they need to construct and secure capacities in cyberspace. Receiving assistance to create frameworks and infrastructure to secure and build capacities in cyberspace are of limited use if the receiving country does not have the capacity to maintain these mechanisms. The challenge is thus to provide capacities than can be utilized at the countries current state. It is imperative to create frameworks and infrastructure that a developing country can maintain. Training local personnel in maintenance of the framework and infrastructure implemented by CCB is a step in the right direction. This gives the country in question independence, so it can generate and uphold its own systems.

5. The private sector owns much of what constitutes the Internet, from routers to infrastructure and technology companies. The private sector thus has the upper hand and knowledge on securing cyberspace. A challenge in any country is for the state to cooperate with the private sector in securing cyberspace. Widely argued for is the need for the private sector to assist the public sector in reaching the same levels of knowledge to secure cyberspace.[9] However, what is less mentioned is the tendency in smaller businesses of the private businesses in developing countries to show a limited interest in investing and implementing cybersecurity. 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. The challenge here is to get the small and medium private-sector actors to understand the costs of not securing their cybersystems. A lack of analytical background for mainstreaming ICT into specific development areas makes implementation and creation of awareness difficult. Education and information sharing is essential for securing cyberspace.

8 Council of Europe 2013 'Capacity building on cybercrime', discussion paper. Data protection and cybercrime division (Strasbourg: Council of Europe)

9 See the United Nations Department of Economic and Social Affairs (2011) 'Cybersecurity: A global issue demanding a global approach' (New York, UNDESA, 2011) and Calandro, E., Gillwald, A. and Zingales, N. (2013) 'Mapping Multistakeholderism in Internet Governance: Implications for Africa', Evidence for ICT Policy Action – Discussion Paper (Research ICT Africa, Cape Town)

Challenges for assisting nations

1. Data
To assist in the implementation of and to improve another country's cyber capacities, a donor country relies on the ability to obtain correct and informed data of the current situation in the country in question. However, collecting and creating such data is challenging, and large datasets are both hard to work with and unreliable. Collecting data through the country receiving assistance is hard as what they choose to present and ask for in assistance is not always what it is they really need, or require. A challenge here is to obtain correct information, so as to be able to assess what aspect of CCB should have top priority.

2. Locating partners
For CCB to be successful, partners on the donor side must work with partners on the receiving end. These partners need to both understand the importance of CCB and have influence at high levels of government. However, it is not always easy to locate these partners, or get cybersecurity and capacity building placed on their agenda. The amount of people in government that have a thorough understanding of the importance of cybersecurity and capacity building is limited, so other developmental projects are given priority over CCB. Further, issues of trust and security measures are involved. This in turn affects the information the donor country receives about the capacities in the recipient country. This impedes good cooperation between the potential partners. The private sector is essential in securing cyberspace, however donor countries need to work through the government of the country it is assisting through development aid. This is challenging as it is up to the developing country to build good relations with the private sector in its country, a matter that is not always in place. More time and attention need to be focused on locating the right partners and creating awareness of the importance of CCB. Here, willingness as well as political stability within the receiving country is essential.

3. Training
Education is needed, in the form of awareness creation and technical education in the field of cyberspace and security. This can provide recipient countries with the capacities they need to secure cyberspace and the related infrastructure. Without this knowledge they risk becoming dependent on donor countries to uphold their own cyber capacities – an unenviable situation. However, one challenge raised in some cyber security forums concerns being able to know that the knowledge shared in high-quality cybersecurity training courses is used to protect the country in question and not to attack others is a risk. Training is essential, but it requires a critical awareness.

4. Communication and cooperation
Clear and frank communication and cooperation among all partners involved in CCB is essential. Donor countries need to communicate amongst themselves and with other organi-

zations that are developing CCB analysis and tools. Equally, good communication with the recipient countries must be established, to ensure that appropriate assistance goes to the countries that need it. Locating countries and organizations that work with developing CCB on the same topic is a consistent challenge. Few forums exist for such communication; and the rapid development and growth of the field make it difficult to keep track of the myriad of actors.

Conclusions and policy recommendations

Cybersecurity must be included in all areas of society: the judicial, social, economic, governmental and educational sectors must all be strengthened to include cybersecurity. Current models and assessments of CCB evaluate national levels of CCB in individual countries, but few are able to provide recommendations for how to improve a country's cyber capacities. Classification is important, but the ability to improve is equally so. This makes possible a firmer, more targeted approach to CCB and allows for assistance, as both the receiving and donor country can know what stage the developing country is in, and thus what needs to be improved. Mapping out the challenges takes CCB one-step ahead towards finding solutions. The challenges are important to discuss and keep in mind when considering the importance of CCB in development aid.

Developing countries will need to deal with challenges in all types of activities connected to CCB – from human resource development, institutional reform, organizational adaptions, to the support provided to increase their access to, and ability to benefit fully from, the Internet and other elements of cyberspace. For CCB to be successful, cybersecurity and laws against cybercrime must be included in the existing legal framework. Further, critical infrastructure needs to be strengthened. With these elements in place, people can utilize the Internet, with the danger of malware and similar threats reduced. It is important for developing countries to aim at making the legal framework feasible but simultaneously broad enough to ensure sufficient legislative reach. However the lack of an analytical background for mainstreaming ICT into specific development areas makes implementation difficult. Awareness creation through education and information sharing is vital for good cyber hygiene and sustainable cyber capacity. This must be done on all levels, from the grassroots to the top echelons, in all departments and sectors, from legislation to the creation of new departments and infrastructure. The ability to communicate this information is a central factor. Educators, means and funds are needed to achieve this goal. Being able to locate the right partners to create awareness of the importance, willingness and political stability is a key factor in building cyber capacities. Education, learning, sharing and cooperation are central to success.

Given the speed of technological progress, it is important to think of capacity building as a dynamic process where the needs of stakeholders are in constant evolution. Mainstreaming various structural and cyber specific 'add-ons' into different policies can promote the development of policies that are more resilient to all types of risks . By assisting in building cyber capacities, donor countries contribute to creating a safe and stable cyberspace, which in return can allow for social and economic development for the county as a whole. CCB is about more than just securing and utilising cyberspace: successful implementation can help to provide broader stability and socio-economic growth. The investment in securing cyberspace is crucial, as it affects the success rate of other policy initiatives as well.

This report is part of the project "Cybersecurity and Developing Countries", funded by the Norwegian Ministry of Foreign Affairs.

Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

About the Author
Lilly Pijnenburg Muller is a Junior Research Fellow in the security and defence group at the Norwegian Institute of International Affairs. Her research focus is on cybersecurity and cyber capacity building, global governance and public private relationships. She holds a MA in politics from the University of Glasgow.
lilly.muller@nupi.no

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PO Box 8159 Dep. NO-0033 Oslo, Norway
www.nupi.no | info@nupi.no