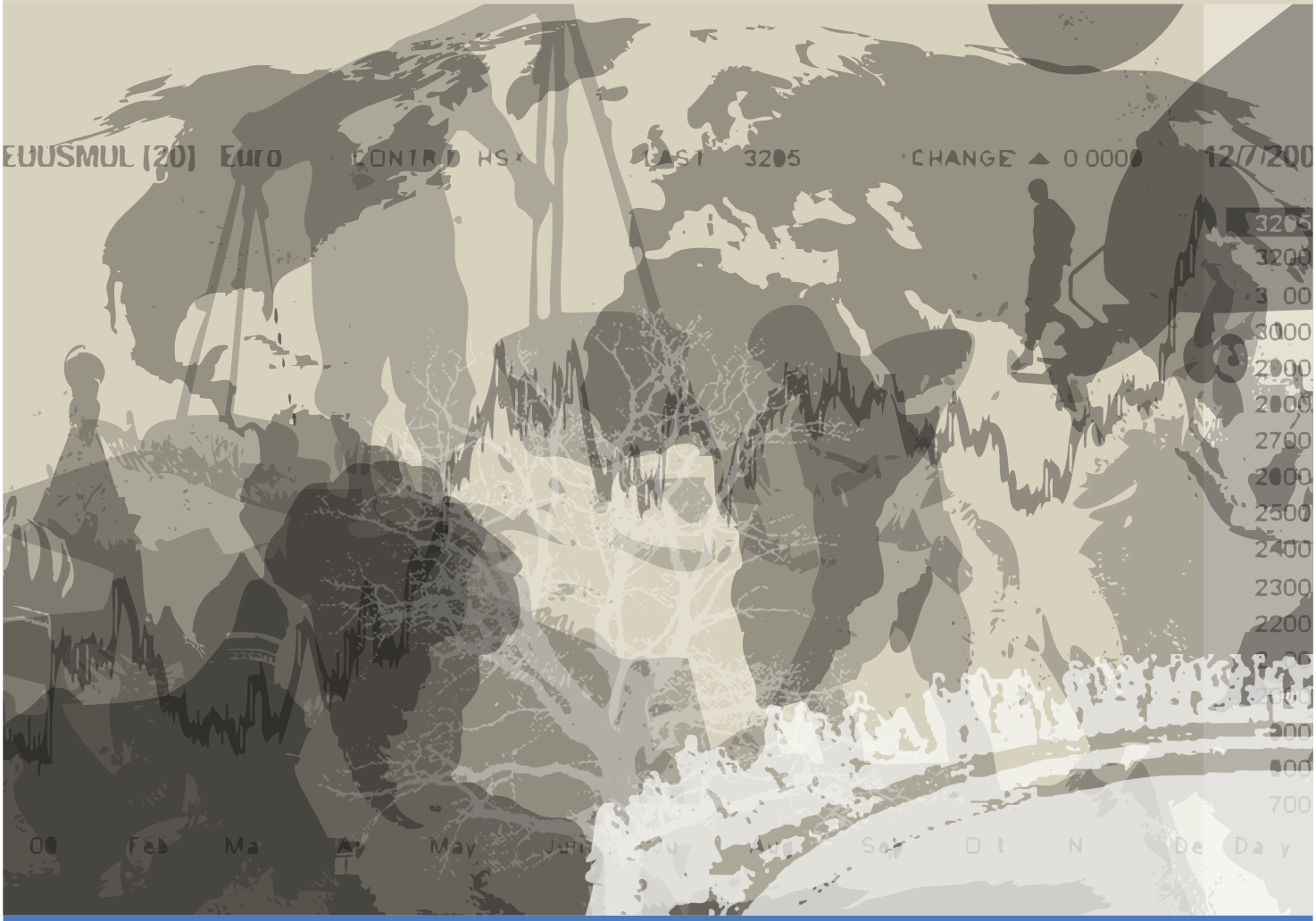
Norwegian Institute of International Affairs

Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities

Lilly Pijnenburg Muller



NUPI Report
[Report no. 3, 2015]

Publisher: Norwegian Institute of International Affairs

ISSN: 1894-650X

Visiting address: C.J. Hambros plass 2d
Address: P.O. Box 8159 Dep.
NO-0033 Oslo, Norway
Internet: www.nupi.no
E-mail: info@nupi.no
Fax: [+ 47] 22 99 40 50
Tel: [+ 47] 22 99 40 00

Cyber Security Capacity Building in Developing Countries: Challenge and Opportunities

Lilly Pijnenburg Muller

Published by Norwegian Institute of International Affairs

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 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 impact on social and economic development worldwide this brief puts forward challenges to implementation. The aim 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.

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

Introduction

Cyberspace is growing at a speed unprecedented by any other commodity. Almost three billion people are now connected to the Internet through cyberspace; a figure growing rapidly and estimated to reach five billion people, using 50 billion devices, by 2020 (Evans, 2011). As most of this growth will take place in emerging economies, it is not surprising that the development community is pondering how to better leverage the benefits accruing from the use of cyberspace and Information and Communication Technologies (ICT) through cyber-capacity building (CCB).[2] This exercise, however, will prove futile unless backed up by serious discussion about the need to address the challenges posed by the proliferation of ICT infrastructure and Internet applications for sustainable development in the implementation of CCB.

Cyberspace is a new environment where no country is immune to the threats that its use entails. With rapid growth come possibilities in development and new ways to empower people: however, this is accompanied by new vulnerabilities, risks and challenges. It is therefore crucial to research how to build cyber-capacities in developing countries and simultaneously how to secure these. Cyberspace and CCB rapid development has resulted in that the literature of and the developments in CCB are sporadic and disordered in nature, which makes keeping up with progress in the field a challenge. This report sets out to collect and assess some of the work conducted to date, and examines its feasibility and applicability. Next, we build on the analysis of this work and give an assessment of what can be built upon for successful implementation. Thirdly we map out some of the general challenges facing CCB on the donor as well as the recipient end. It is important to chart these: if the challenges can be quantified, then solutions to bring CCB forward can be proposed. Given the rapid pace of technological progress, capacity building must be recognized as a dynamic process where the needs of stakeholders are constantly evolving. Nevertheless CCB is essential; a firm and targeted approach is called for. It is of paramount importance to invest in securing cyberspace, as this affects the success rate of other policy initiatives. This report takes a step towards implementation of CCB by specifying the challenges for the road ahead.

---

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.

Cybercapacity building in developing countries

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 (ITU, 2014). Cyberspace is an intrinsic part of the development of any country. A strong cyber capacity is crucial for states to progress and develop in the economic, political and social spheres. It is therefore essential to mainstream CCB into development programs so that countries can get the assistance they need to improve and secure their development and growth (ISSEU, 2013; UNDESA, 2011, UNIDIR, 2013).

To build a stable and solid cyber capacity the capacities built to utilize cyberspace need to be secured. Cybersecurity in this report is defined as the response to threats to a well-functioning cyberspace through the empowerment of individuals, communities and governments.[3] This is crucial for achieving a country's developmental goals, as it reduces the digital security risks stemming from access to and use of cyberspace. A This broad view of 'risks' is taken in this report to include not only those posed by 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 programs, content blocking) (Pawlak 2014). Consequently we employ the term CCB throughout this report as an umbrella concept for all types of activities (e.g human resource development, institutional reform, organizational adaptions) and support provided to developing nations to increase their access to, and ability to benefit fully from, the internet and other elements of cyberspace (ibid., EUISS 2014)

As cyberspace knows no boundaries, developing countries increasingly face the same cyber threats in cyberspace as the developed world does in correlation with their increasing access and use of cyberspace. These threats range from malware to cyber-crime, in the form of attacks

3 Such threats can come from various kinds of malware: an attack on different forms on the codes that make up cyberspace. When these codes are changed by actors other than those who 'own' them or have created them, we talk about an 'attack'. Such attacks may involve spying on, stealing, abusing and destroying digital information, in extreme situations creating physical and off-line effects. The different ways of altering a code are what separates the different viruses and attacks on cyberspace, but the core point is that what is involved is unauthorized change to code (Cavelty, 2014). Another form of vulnerability is systemic failures as a result of malware, as with blackouts or loss of control of vital control systems.

on state infrastructure, vital industry, information technology and individuals (UNDOC, 2013; ITU, 2012). As proper network, security and legal framework often lacks in developing countries they have fewer capabilities for dealing with these challenges than the developed world (IDG connect, 2012). This makes them vulnerable to cybercrime and increases the chances of being attacked. Further the countries governmental institutional capacity and awareness of the threat is often limited.

Awareness of the extent to which cyberspace vulnerabilities and limited capacities prevent countries from maximizing the benefits stemming from the use of the Internet has started to emerge slowly in some countries, but they often suffer from limited resources or lack of experience. Struggling with pressing issues directly linked to social and economic development, most developing countries welcome the 'digital wave' as an opportunity, without paying sufficient attention to the associated risks (Pawlak 2014). Others show increasing scepticism to the measures needed to protect and secure the digital realm, seeing them as 'Western imposition' on their governance. The result is that developing countries are rapidly increasing their access to cyberspace, without adequate security measures. This can bring in more damage than benefit to both the state and the local economy (Burt et al. 2014a). Progress is inseparably linked with IT and technology, but it requires the right support apparatus. That is why CCB 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 developing nations on cyber capacity. Finding the right way to do this in practice is another matter.

Cyber capacity building today

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). The differences in focus result in fragmented coverage of CCB; moreover, the size of the field, unreliable data and rapid development in cyberspace itself may lead to insufficient approaches and methods. Methods to date have not managed to cover CCB as a whole on a global scale – or else they argue for CCB, but without indicating how to go about implementing it. Some approaches set out a scope that is either too broad or too narrow, while others focus on different ways of highlighting the problems that come with increased access to cyberspace, but without indicating solutions. Nevertheless, some trends are emerging in the international CCB policy debate as to how to provide developing nations with increased access to, and the ability to benefit fully benefit, the Internet and cyberspace more generally. Common features here are improved social and economic conditions through increased security, legal frameworks or other means; however, reports and arguments vary widely on how to achieve these.

Recent reports have shifted focus from the broad overall scope and arguments concerning CCB and argue that CCB programs must be firmer and precise to be successful. This entail creating a holistic approach, often encompassing five areas of society: the judicial, social, economic, governmental and educational sectors. In this way, the complexity and encompassing nature of cyberspace is split up, making the work and analysis approachable and allowing the objective to be explicitly defined.

With their *Cyber Index the UN Institute for Disarmament Research* (UNIDIR 2013) take a step towards mapping out the technical/political levels of the cyber capabilities of individual countries, organizing all countries according to the level and structure of their cyber capacity and security. However, countries' capacities are mapped out individually in this index, minimizing the ability for comparison. Further, the model is not open to adaptability and moulding depending on changes and improvements in country capabilities. Once a country has been entered in the Index, changes are not included. This limits its applicability and the use of the classification in assistance and CCB.

Another index that works towards a firm and precise cyber capacity analysis is the *Cyber Readiness Index 1.0* created at the Belfer Center at Harvard University. This index maps 35 countries that have embraced ICT and the Internet, and then applies an objective methodology to evaluate each country's maturity as to its commitment to cybersecurity across five essential elements.[4] This work is crucial for CCB; as aiding countries through this index can evaluate who they can assist and how. Nevertheless the index to date is limited by the number of countries included, restricted by the number of countries included in the index.

To circumvent the restriction of number of countries that a analysis can thoroughly examine the Australian Strategic Policy Institute, with its *International Cyber Policy Centre Maturity Metric (2014)* assesses the regional cyber-landscape and evaluates whole-of-government policy and legislative structures, military organization, business and digital economic strength and levels of cyber-societal awareness in the Asia-Pacific region. Also noteworthy is Cyber Green (2014), recently launched by the *Asia Pacific Computer Emergency Response Team network,* aimed at establishing an effective hub for collaboration efforts to address cyber risks and improve the health of the cyber ecosystem. However, both the above-mentioned initiatives are limited by their regional focus. Regional assessment is useful, but as cyberspace has no boundaries, the issues these countries faces are not always regionally defined. A country in another region might have more in common in its cyber capacities and challenges it faces with a country in a different region than a neighbouring country. Excluding this comparison thus restricts the development of CCB.

Taking a step towards global assessment Microsoft, one of the private stakeholders with the most information on cybersecurity, has sought to move CCB forward by creating several models and classification systems based on their own data. The most recent approach, *Linking Cybersecurity Policy and Performance* (Kleiner et al. 2014), provides a comparative classification system where various levels of the cyber capacity of nations are compared. Acknowledging that all countries differ in their capacities, the creators of this model also attempt to identify similarities. Based on an assessment of the relationship between the prevalence of malware combined with an analysis of socioeconomic factors and policy choices, countries are sorted into three distinct clusters: maximizers, aspirants and seekers.[5] This allows for assessment of the links between changes in national development and cybersecurity over time, as well as a focus on how

4 The successor 2.0 is under development and will include 125 countries in the analysis

5 The work is based on a statistical model that includes 80 social and economic policy indicators. Using 34 of these (including GDP/cap, literacy rate, and rule of law) it aims to predict a country's malware by tracking infection rates of malicious software (malware) and then using this as a proxy to measure cybersecurity performance (Kleiner et al. 2014).

cybersecurity is changing. Tracing malware is a useful and promising approach. Equally, the ability to assess developing countries' malware is helpful for analysing the extent and nature of cybercrime in developing countries.

Taking another approach the *Organization of American States* (OAS) and the *International Telecommunication Union* (ITU), together with the International *Multilateral Partnership Against Cyber Threats* (IMPACT) map cybersecurity levels of their member states through organized exercises and 'cyber-attacks' or 'hosted regional cyber-drill exercises'. Through these they can map out what capacities the countries have and direct visualization of what the countries in question lack as regards to cyber capacities. Further these exercises provide an understanding of the harm and risk of having limited cyber capacities. However, these exercises are limited by their ability to target only certain aspects of a state, leaving the private sector excluded. Further they do not provide the countries with the ability to improve their situation.

The Global Cyber Security Capacity Centre (GCSCC) at Oxford University has taken a step towards closing the gaps between the work of these institutions, with the creation of the *Cyber Security Capability Maturity Model* (CMM). Though still only a pilot model, it aims to allow countries to self-assess their level of cyber capacity and then directly receive information on how to make improvements. This is done by the governments of the state applying information to the model, responding to direct and straightforward questions concerning their cyber capacities. The aim of the model is to focuses broadly, dividing its span of analysis into five pillars of society.[6] These are (1) devising cyber policy and strategy (2) encouraging responsible cyber culture in society (3) build cyber-skills into the workforce and leadership (4) create effective legal and regulatory frameworks (5) control risks through organizations, standards and technology. Any country, independent of its capacity level, can use this tool. Based on their answers and on how they score in self-assessment, counties are classified in one of five levels: (1) Start-up: embryonic, (2) Formative: 'new', (3) Established: indicators are functional and defined, (4) Strategic: choices have been made about what to prioritize, (5) Dynamic: rapid decision- making, reallocation of resources and constantly changing environment. Depending on where a country stands according to its self-assessment, the GCCES tool then proposes the next steps that need to be taken to improve its cyber capacity. This means that instead of placing countries in a cluster based on what they lack, it is possible to assess what they have, and automatically inform them on what they need to strengthen and improve the situation. The more frank a country is in its self-assessment the more will it benefit. The classification is useful as it allow for an assessment of countries cyber abilities and capabilities and

their capacity to handle cybersecurity threats. This allows for a firmer and targeted approach to CCB and brings us closer in being able to assist developing countries in their CCB. Further it allows for assistance, as both the receiving and donor country know what stage the developing country is in, and what needs to be improved to advance the developing countries cyber capacity. However this model is still in the developmental phase.

Implementation and the ability to provide countries with what they need to strengthen and improve their CCB, and how to link these results to donor countries, are problems that remain unresolved. Nevertheless the assessment of the work done to date in CCB shows that solid steps are taken towards successful assessment, mapping and comparison of countries cyber capacities. This allows for analysis of countries cyber capacities and thus of the levels of the individual countries cyber capacity. However implementation is still a challenge. To move the field forwards the next section in this report will map out some of the main challenges to CCB, both on the donor and recipient end. It is important to emphasize that all countries face different challenges in implementing CCB. Mapping out the challenges to CCB in a country or a region requires the recognition of the specificities of a given context (i.e. cultural, political and social heritage) and needs to ensure local ownership. While individual components of challenges are case specific, similar challenges can be found and the overall approach and objectives can be replicated. For instance, even though responsibilities can be assigned differently depending on the country in question, challenges often remain similar (ISSEU, 2014). As argued at the international conference on cyber capacity building in Paris in 2014: 'One size does not fit all, however one size fits most' (ISSEU, 2014:2). To move CCB a head challenges need to be mapped out for capacity building to move towards implementation.

Way ahead and challenges for CCB

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 shaped by Western donors are less likely to prove sustainable. Classical dilemmas in the development sector related to sustainability and local ownership are equally relevant to CCB.[7] 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. To simplify, these are divided into challenges for donor and developing countries, but in practice they are all interconnected and influence each other.

Challenges for developing countries

Developing countries face challenges in all types of activities connected to CCB – from human resources development, institutional reform, organizational adaption, and in the support provided to increase their access to, and ability to fully benefit from, the Internet and other elements of cyberspace. These challenges make it difficult to secure cyberspace and the outcome of implementation.

1. Access versus institutional stability

Access to cyberspace is growing faster than the institutions and frameworks that states use to support it. This growth in access is positively received in the developing countries as it allows more people to connect to cyberspace and the Internet which in turn is seen as a to boost the economy (Burt et al. 2014a). However without institutional stability and legal frameworks, increased access can create more damage than benefits (IDG connect 2013). People become an easy target for cybercrime when there is no framework or institution to prevent it. The challenge is to create a structure and institutional stability that can allow for utilization of the Internet, while simultaneously guarding the users against malware threats, which increase with access to cyberspace. To this end, critical infrastructure must be strengthened and efforts made to include cyberspace in existing legal frameworks. It is essential for the country in question to have a clear understanding of its own capabilities and equally of what needs to be strengthened. Occasions are found where countries ask for assistance in areas other than what should in fact be prioritized for sustainable cyber capacity.

---

7 The idea of 'local ownership' was established as a principle in 1996 by the Development Assistance Committee (DAC) of the Organization for Economic Co-operation and Development (OECD). In what is often regarded as a seminal report DAC stated: 'the most important contributions for development, as in the past, will be made by the people and governments of the developing countries themselves' (DAC, 1996).

For example, a county may ask for assistance to build a CERT – but without having the capacity, or knowledge, to uphold one. The challenge is for developing countries to obtain a clear overview of what institutional and structural capacities they have, and that they have an understanding of what they need in order to achieve and improve their cyber capacity. Equally important is sharing this information with the aiding country or organization, to allow for efficient and sustainable institution and structure building.

2. 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 (Council of Europe, 2013). A functioning legal framework makes it possible to regulate governance, punish crimes, and control implementation in cyberspace. 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. This is seen in the contested debate around the new convention of the African Union (AU) on Cyber Security and Personal Data Protection that requires African states to 'establish appropriate institutions to combat cybercrime' and to offer training to those stakeholders tasked with fighting cybercrime' (AU Convention, EX.CL/846 XXV: 30). This is to be built into all aspects aimed at improving the legal and judicial aspects of cybercrime and security. However, concern has been voiced in that it is overly ambitious and too cumbersome. It has been questioned whether the convention asks too much of the AU member countries (Tamarkin, 2015). On the other hand, this new convention can function as a guideline and goal, as something for the AU members to aim for and support, instead of undervaluing it and putting it aside. True, 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.

3. Affordability

Many countries *lack resources to build what they need* to construct and secure capacities in cyberspace. Implementing frameworks and infrastructure is of limited use if the receiving country does not have the capacity to maintain it. According to the UN Economic Commission for Africa (UNECA), African governments demonstrate an increased awareness of cybersecurity issues, but existing capacity for deterring cybercrime and monitoring or pursuing cybersecurity has been ineffective (IDG connect 2013). The New Partnership for Africa's Development (NEPAD) is charged with developing and implementing a capacity-building project that works to close gaps in AU expertise and training. The main challenge has been lack of funding for the work (Caladro et al 2013). It is thus 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, to generate and uphold its own systems.

4. 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. Without awareness and education the effort to secure a system is rendered inefficient if not useless (Tamarkin, 2015). 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. This is a widespread problem for all levels society in many developing countries – from the general population and grassroots to government (UNODC 2013). Training should be provided both 'vertically' and 'horizontally' across government departments, the involved private actors and civil society (ISSEU 2013). The challenge is how to spread information and understanding of cyber hygiene. Awareness building is difficult if cybersecurity is not a government priority. A comprehensive understanding of the security and technological challenges is needed within governments. Otherwise, implementation of cyber security becomes difficult. Otherwise, implementation of cybersecurity becomes difficult. This lack of understanding and knowledge may also create conflicts of interest within governments. When only some sections in various government ministries and agencies recognize the importance of cybersecurity, implementation becomes difficult and slow. People become frustrated at the cumbersome processes of moving legislation ahead. Further complications for CCB arise in the number of stakeholders that need to be engaged in both the public and private sphere. A challenge is the need to be proactive in risk management, and at the same time conveying an understanding of the overall purpose that the security measures are intended to serve. Lack of understanding and knowledge on how to improve cyber capacity limits its further development.

5. Public-private cooperation

The private sector owns much of what constitutes the Internet, from routers to infrastructure and technology companies. The need to strengthen cooperation between the public and private sector in order to obtain a strong cybersecurity is widely argued for (UNIDIR, 2013; UNDESA, 2011; Calandro et al. 2013). Such a public private partnership models needs to be created in the country building its cyber capacities as the private industry owns much of the ICT infrastructure and is most active in the development of new technologies (EUISS 2013). However a second challenge in this debate is one seldom mention; that of the small and medium size private business in developing countries that also largely depend on cyber technologies, in the form of computers and internet. These businesses tended to show low interest

in implementing and investing in cybersecurity. The issue here is a twofold. Firstly there are the firms who sell 'cybersecurity' in the form of software to these companies that the buyers do not understand. Without an understanding of how to use such software, its effect becomes limited. And secondly, there are businesses owners that acquire software that they know do not uphold recognized standards (as pirated software), in order to avoid legal penalties. This software does not provide the security they need– but it keeps them 'safe' from the legislation that requires businesses to have software to protect their computers. Both these challenges result in a less secure Internet, locally as well as globally. 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 these private sector actors to understand the costs of not securing their cyber-systems. 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.

Challenges for assisting nations

The challenges in securing cyberspace in developing countries are found not only in the countries receiving assistance, but on the donor side as well. These need to be mapped out and taken into consideration for a successful CCB. By assessing the challenges on the donor side in CCB we move the debate one step closer to implementation.

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. Because of the security challenges involved, the amount of information the hosting country is willing to share will vary. The countries in question do not always want to share nor do they always know exactly what capacities they have, or need. This in turn affects their ability to judge what capabilities are most essential for them to build. Thus what they choose to present and ask for in assistance is not always what it is they really have, 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. A second challenge is to 'convince' countries of what they do need, based on the information they share, without imposing 'Western concepts'.

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 the agenda. If the assisting country is to work through development aid it needs to work with the government of the country it is assisting. However the public sector is found to lack a thorough understanding of the importance of cybersecurity and capacity building, so other developmental projects are given priority over CCB. Further, issues of trust and security measures are involved when the donor country receives limited information about 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

Training of key stakeholders in developing countries and providing them with the capacities they need to uphold cybersecurity is important for a stable cyber capacity. Without the knowledge and ability to maintain cybersecurity, a developing country's cyber capacity is limited. 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. It is vital that recipient countries receive the training needed to be able to control and upkeep the capacities built through CCB programs. 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. When donor countries share their knowledge and ability to protect their systems, with the aim of allowing other countries to do the same and build functional CERTs to fend off cyber-attacks, they also give the knowledge of how to attack the systems of other countries. This is a recognized dilemma encountered in connection with training police and military in developing countries in peace and stabilization operations. The challenge here is to come to an understanding on how to educate and give training in cyber capacity and security. Having a clearly defined and unifying objective can remove many obstacles and provide the premises for more efficient cooperation. One should focus first on creating awareness and understanding of the problems that come with cyberspace in all its forms, in all the levels and branches of the state, before giving technical training. 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 organizations 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. The rapid development of cyberspace and the lack of communication channels among donors and between donors and recipient countries encumber this process. Poor communication channels between the actors involved may result in overlapping and duplication of work. 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. The newness of the field, combined with its rapid development and the state security aspects, obstructs openness and a culture of sharing. This affects the development of the field on both ends. The developing countries receive conflicting messages and uncorrelated aid from a range of different donor countries, creating confusion and hindering the development of cyber capacities. Poor communication among donors affects the outcome and success rate of CCB in the whole. With differing focus areas and solutions to the problem, resources are not put to best use.

Conclusions

This report has collected and assessed work conducted to date on CCB, to examine its feasibility and usefulness in bringing CCB ahead towards successful implementation. Our assessment shows that a holistic model is needed. The focus cannot be solely on one area, but must include all areas of society: the judicial, social, economic, governmental and educational sectors. Current models and assessments of CCB are successful in evaluating national levels of CCB in individual countries, however the ability to aid countries in how to improve their cyber capacities is still lacking. The Oxford GSCSSs pilot model arguably takes a step in the right direction as it allows for full assessment of a country's capacity, while remaining flexible and able to provide direct responses on how to improve these 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.

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. 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. It is important to emphasize that all countries face different challenges in implementing CCB. Mapping out the challenges to CCB in a country or a region requires the recognition of the specificities of a given context (i.e. cultural, political and social heritage) and needs to ensure local ownership. However while individual components of challenges are case specific, similar challenges can be found and the overall approach and objectives can be replicated. This report has mapped out some off the general challenges that all countries face, albeit in different degrees.

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 a good cyber hygiene and sustainable cyber capacity. This is important both in the private and public sector, from the grassroots to the top echelons. In the state system all departments and sectors need to be better informed. The ability to communicate this information is a central factor. Educators, means and funds are needed to achieve this goal. Education, learning, sharing and cooperation are central to

success. 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. Further cybersecurity and laws against cybercrime must be included in the existing legal framework. The challenge is to create a critical infrastructure and institutional stability as early as possible and to integrate this into the local system, to allow maximal utilization of the Internet and secure its users against malware. These elements in place allows for utilization of the Internet with a lower risk of danger of malware and similar threats.

The investment in securing cyberspace is crucial, as it affects the success rate of other policy initiatives as well. Assistance is essential to developing countries that are expanding their access, their capacity to use cyberspace and their overall development and security. 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 may promote the development of policies that are more resilient to all types of risks (Calandro and Pawlak 2014). By assisting in building cyber capacities, donor countries contribute to creating a safe and stable cyberspace. CCB is about more than just securing and utilising cyberspace: successful implementation can help to provide broader stability and socio-economic growth. A focus on private-public cooperation, education, governance, policy and national strategy in CCB is recommended. This report has taken a first step towards implementation of CCB by mapping out the challenges for the road ahead. What is needed next is a comprehensive analysis of the challenges and recommendations for advancing CCB.

References

African Union Convention On Cyber Security And Personal Data Protection Ex.Cl/846 (Xxv) opened for signature 27 June 2014. Available at: http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf [Accessed: 5 April 2015]

Asia Pacific Computer Emergency Response Team (2014) 'The Cyber Green Initiative: improving health through measurement and mitigation', Concept Paper (Japan: Japan Computer Emergency Response Team Coordination Centre).

Australian Strategic Policy Institute (2014) 'Cyber Maturity in the Asia–Pacific Region' (Australia: Australian Strategic Policy Institute).

Burt, D., Nicholas, K.S., Scoles, T. (2014a) 'The cybersecurity risk paradox: impact of social, economic, and technological factors on rates of malware', Microsoft Security Intelligence Report Special Edition (SIR), Microsoft Corporation.

Burt, D., Kleiner, A., Nicholas, J.P., Sullivan, K. (2014b) 'Cyberspace 2025: navigating the future of cybersecurity policy', Microsoft Corporation. Available at: http://www.microsoft.com/security/cybersecurity/cyberspace2025/ [Accessed: 7 April 2015]

Cavelty, M., D. (2014) ' Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities' (Zurich: Springer Science)

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)

Calandro, E. and Pawlak, P. (2014) 'Capacity building as a means to counter 'cyber poverty,' in Pawlak, P. (ed.) *Riding the digital wave the impact of cyber capacity building on human development* (Paris: ISSUE)

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

Council of the European Union (2013) '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

Development Assistance Committee (DAC) (1996) 'Shaping the 21st Century: The Contribution of Development Co-Operation ' (Paris: OECD).

Ericsson (2014) 'Sub-Saharan Africa: Ericsson mobility report appendix'. Sony Ericsson. Available at: http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-ssa.pdf [Accessed: 1 April 2015]

European Commission (2013) 'Cybersecurity strategy of the European Union: An open, safe and secure cyberspace', Brussels, 7 February

European Union Institute for Security Studies (EUISS) (2014) 'Cyber Capacity Building in Ten Points' note based on deliberations during the international conference on cyber capacity building hosted by the EU Institute for Security Studies (Paris: EUISS)

Evans, D. (2011) 'The Internet of Things How the Next Evolution of the Internet Is Changing Everything'. Cisco white paper Cisco Internet Business Solutions Group (IBSG)

Global Cyber Security Capacity Centre (GCSCC) (2014) 'Cyber Security Capability Maturity Model (CMM) – Pilot, Oxford University'. Available at: http://www.sbs.ox.ac.uk/cybersecurity-capacity/content/gcscc-cyber-security-capability-maturity-model-cmm-0 [Accessed: 1 April 2015]

Hathaway, M. (2013) 'Cyber Readiness Index 1.0'. Paper, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Kennedy School of Government at Harvard University, 8 November.

IDG connect (2013) 'Cybercrime, hacking and malware'. IDG Connect. Available at: http://www.idgconnect.com/download/11401/africa-2013-cyber-crime-hacking-malware?source=connect [Accessed: 12 April 2015]

ISSEU (2013)'Capacity building in cyberspace: taking stock'. A seminar organised in the framework of the EUISS Cyber Task Force Event Report (Brussels, EUISS, 2013).

International Telecommunication Union (ITU) (2014) 'The World in 2014 ICT facts and figures' (Geneva: ITU)

ITU (2012) 'Tracking four years of achievements: implementing the Hyderabad Action Plan' (Geneva: ITU).

ITU (2014) 'World Telecommunication/ICT Indicators database', 18th edition. Available at: http://www.itu.int/en/ITU-D/Statistics/Pages/publications/wtid.aspx [Accessed: 7 April 2015]

Kleiner, A. Nicholas, P. Sullivan, K. (2013) 'Linking cybersecurity policy and performance', Microsoft: Microsoft Trustworthy Computing Available at: http://www.ilsole24ore.com/pdf2010/SoleOnLine5/_Oggetti_Correlati/Documenti/Tecnologie/2013/02/SIR-Special-Edition-Security-Atlas-whitepaper.pdf [Accessed: 7 April 2015]

MDG Gap Task Force Report (2009) 'Strengthening the Global Partnership for Development in a Time of Crisis'(New York: United Nations).

Microsoft (2014) 'Microsoft Security Intelligence Report' (MSIR) Volume 17 Available at: www.microsoft.com/sir [Accessed: 1 April 2015]

Organisation for Economic Cooperation and Development (OECD) (2012a) '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

Organisation for Economic Cooperation and Development (OECD) (2012b) 'The role of the 2002 Security Guidelines: towards cybersecurity for an open and interconnected economy', OECD Digital Economy Papers, no. 209.

Organisation for Economic Cooperation and Development (OECD) (2014) '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 (Paris: OECD).

Organization of American States and Symantec (2012) 'Latin American and Caribbean Cybersecurity Trends', June 2014. Available at: http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf [Accessed: 1 April 2015]

Pawlak, P. (2014) 'Developing capacities in cyberspace', in Pawlak, P. (ed.) *Riding the digital wave: The impact of cyber capacity building on human development*, ISSUE, report nr 21.

Porcedda, M.G (2014) 'Rule of law and human rights in cyberspace' in Pawlak, P. (ed.) *Riding the digital wave: The impact of cyber capacity building on human development*, ISSUE, report nr 21.

Tamarkin, K. (2015) 'The AUs cybercrime response' the institute for security studies, policy brief 73. Available at: http://www.google.no/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.issafrica.org%2Fuploads%2FPolBrief73_cybercrime.pdf&ei=VsUqVbrtKcaTsgGn2oCoDg&usg=AFQjCNGYkwZPBWArcX6Ogl4OOCoxjMVUvw&sig2=jb2hYTLeKtBPsiMxuf5Asg&bvm=bv.90491159,d.bGg [Accessed: 10 April 2015]

United nations Institute for Disarment research (UNIDIR) (2013) ' The Cyber Index Internatioanl Secuirty Trends and Realities' (UNIDIR, Geneva)

United Nations Department of Economic and Social Affairs (2011) 'Cybersecurity: A global issue demanding a global approach' (New York, UNDESA, 2011) Available at: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html [Accessed: 1 April 2015]

United Nations Development Programme (2013) 'ICTs and e-governance in UNDP: 2013 Status Report'. Available at: http://www.undpegov.org/sites/undpegov.org/files/e-gov-Mapping-2013-10-28_0.pdf [Accessed: 6 April 2015]

United Nations Development Programme (2014) 'Human Development Report 2014. Sustaining Human Progress: Reducing Vulnerabilities and Building Resilience'. Available at http://hdr.undp.org/en/2014-report/download [Accessed: 1 April 2015]

United Nations Economic Commission for Africa (2015) 'Capacity Development', Available at: http://www.uneca.org/our-work/capacity-development [Accessed: 1 April 2015]

United Nations Institute for Disarmament Research (UNIDIR) (2013) 'The Cyber Index International Security Trends and Realities' (Geneva: UNIDIR)

United Nations Office On Drugs and Crime (UNODC) (2013) 'Comprehensive study on cybercrime: draft' – February 2013, 178. Available at: http://www.google.no/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB4QFjAA&url=http%3A%2F%2Fwww.unodc.org%2Fdocuments%2Forganized-crime%2FUNODC_CCPCJ_EG.4_2013%2FCYBERCRIME_STUDY_210213.pdf&ei=7MUqVZ1GzJ-yAdqVgPgL&usg=AFQjCNFoJTRP-

PIsyx__BHuRMx7J-JPBvQ&sig2=Gq0G6Wjj-wyr3q4rbHDpfQ&bvm=bv.90491159,d.bGg [Accessed: 1 April 2015]

Wahito, Margaret (2012) 'Kenya: 20 Percent of Computers Virus Prone' Available at: http://allafrica.com/stories/201206080071.html [Accessed: 1 April 2015]

World Bank (2013). 'World Development Report 2014. Risk and Opportunity: Managing Risk for Development' (Washington, DC: World Bank)

World Bank (2014) 'ICT for greater development impact'. Information and Communication Technology (Washington, DC: World Bank)

World Economic Forum (2012) 'Risk and Responsibility in a Hyperconnected World – Pathways to Global Cyber Resilience'. Available at: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report2012.pdf [Accessed: 4 April 2015]

World Economic Forum (2014) 'Risk and responsibility in a hyperconnected world – Implications for enterprises'. Available at: http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf [Accessed: 4 April 2015]

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

Norwegian Institute of International Affairs

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

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