GPPi
GLOBAL PUBLIC POLICY INSTITUTE

Advancing Cybersecurity Capacity Building

Implementing a Principle-Based Approach

By MIRKO HOHMANN, ALEXANDER PIRANG, THORSTEN BENNER

PUBLISHED
March 2017

Governments, international organizations, and non-state actors all recognize that cybersecurity capacity building (CCB) is crucial to mitigating the negative cross-border externalities of increasing connectivity and maximizing the benefits of ICT-led development. While early adopters have lent support and resources to CCB, the present supply falls short of what is needed to take cybersecurity from an afterthought to an integral part of expanding connectivity. To help close this gap, we present five principles that can provide guidance on scaling CCB going forward. For each principle, we suggest a goal, analyze the status quo, and provide recommendations for how to work towards that goal. The success of these efforts also depends on political leadership, which will be key to utilizing both cybersecurity expertise and existing knowledge and experience on how (not) to build capacity abroad.

The authors owe a special debt of gratitude to the over 40 experts and practitioners who took the time to participate in the individual interviews that form the basis of this report. In addition to the interviews, a review of the slowly expanding literature on cybersecurity capacity building laid the foundation for the report's conclusions.

The authors also thank Josefhine Chitra, Carl Michaelis, and Svea Windwehr for their help throughout the process of creating the report; Maria Bada, Belisario Contreras, Rahel Dette, Julian Lehmann, Claudia Meier, Taylor Roberts, Philipp Rotmann, Isabel Skierka, and Carolin Weisser for their constructive criticism; Maddie Wells for her editing; and Oliver Read for design and overseeing the editing process.

The International Cyber Policy Coordination Staff at the German Federal Foreign Office provided financial support for research for this paper. The authors also thank Karsten Geier and Christian Senninger for sharing their expertise with them. The views expressed in the paper are only those of the authors.

Table of Contents

Executive Summary

Information and communication technologies (ICTs) have become critical catalysts for sustainable development. Yet no country will be able to reap the full potential of ICTs without also building cybersecurity capacity to address the risks associated with connectivity, such as losing trust in digital infrastructures, cybercrime, or even threats to national security. Still, in many nations, and especially those in the process of developing their ICT infrastructures, security often remains an afterthought. But increasing cybersecurity capacity is not only in the interest of individual countries – in a globally connected world where vulnerabilities in one country create risks for others, building resilient systems is crucial. Cybersecurity capacity building (CCB) is key to both mitigating these negative cross-border externalities and maximizing the benefits of ICT-led development.

Cybersecurity Capacity Building Today

Cybersecurity Capacity Building refers to a set of initiatives that empowers individuals, communities, and governments to reap potential gains from investments in digital technologies, or what the World Bank calls "digital dividends." To do so, an engaged community of experts has formed to set up computer security incident response teams, provide support in developing national cybersecurity strategies, and carry out awareness-raising campaigns, among other initiatives. A number of maturity models have been developed to assess and benchmark cybersecurity capacity, and the Global Forum for Cyber Expertise (GFCE) was created as a first attempt to exchange and pool international expertise on CCB.

Early adopters in governments and international organizations as well as non-state actors have increasingly recognized the relevance of CCB to address the risks of connectivity: states such as the UK, Netherlands, or the US, international and regional organizations including the OAS, ITU, and the EU and other actors like Oxford University or Microsoft are slowly lending support and resources to building capacity. For some, CCB has even become a tool for foreign policy – as a means to advocate for a particular model of internet governance, create market access for domestic companies, or promote specific technical standards.

Despite international recognition and an increasing number of incentives, the present supply falls short of what is needed to transform cybersecurity from an afterthought into an integral part of expanding connectivity. Efforts are often under-funded and uncoordinated – both within and between countries – and only few lessons learned and best practices are available. There is little exchange, let alone integration, between cybersecurity and development actors as well as diplomats. As a result, awareness of capacity building pitfalls that have plagued efforts in other areas is increasing slowly.

Five Principles to Address Current Gaps

To help close aforementioned gaps in ongoing efforts and to provide guidance on scaling CCB going forward, we advocate for a principle-based approach. Based on interviews we conducted with over forty experts in the field as well as a broad literature review, we suggest the following five guiding principles: national and international **coordination and cooperation; integration** of cybersecurity and development expertise; **ownership** of the recipient-country; **sustainability** of efforts; and continued and mutual **learning**.

For each of the principles, we suggest a goal – that is, an ideal set-up –, analyze the status quo, and provide recommendations on how to work towards the goal. Our key take-aways are:

For better coordination and cooperation, we urge governments to develop an explicit national CCB approach to enhance the prioritization of efforts, streamline the domestic institutional setup across actors and work with civil society, academia, and the private sector to build efforts on a broad basis. Globally, it is important to push for the strengthening of an international forum, such as the GFCE, to enable cross-sector communication and knowledge exchange regarding efforts and best practices. When it comes to planning specific projects, regional organizations are key catalysts.

To integrate efforts between different communities, cybersecurity and development experts must step outside their respective silos. This can include simple steps such as addressing differences in terminology. While projects and areas of work can remain separate, it should be clear that both work towards a similar goal, ideally in joint projects.

To improve ownership, we urge international actors to develop strategies along with recipient countries and – where possible – ensure high-level and sustained institutional backing. Maturity assessments, such as the Cybersecurity Maturity Model (CMM), can play an important role in not only benchmarking existing capacity, but also bringing together relevant national stakeholders for conversation on CCB.

To ensure the sustainability of efforts, CCB projects need to explicitly define who needs what capacity for what purpose. This trifold approach borrows from existing capacity building practices. As such, there is an opportunity not to start from scratch, but rather take inspiration from capacity building expertise in other areas, as well as established methods and instruments.

Finally, to ensure continued and mutual learning about which measures have (not) worked and why, there is a need to increase the transparency of outcomes and improve models for measurement as well as evaluation. At the same time, a lack of examples and best practices should not deter action; rather, at this early stage, more projects need to be carried out, with learning happening in the process.

The Need for Political Leadership

As these recommendations show, there is an opportunity to make use of both cybersecurity expertise and existing knowledge and experience on how (not) to build capacity abroad, especially in the cybersecurity, development and diplomatic communities. However, CCB currently lacks the necessary top-level leadership

attention and support to seize this opportunity. Depending on the direction that leadership takes, CCB will either "muddle through" or "keep pace"– two plausible scenarios that we develop at the end of the study. In both, exponential growth in connectivity appears to be a given; less certain is how cybersecurity capacity will evolve.

Germany is one of the countries that is well placed to take on a key role in the field. While current efforts are still at a nascent stage, Germany has one of the world's most advanced ICT systems, boasts a strong international network, and can draw upon capacity building efforts in other areas. First, Germany should lead by example in terms of its domestic setup. This means devising a clear strategy that cuts across the turf concerns of different organizations and involves government and non-government actors alike. In parallel, a discussion needs to take place on how to mobilize funding – a conversation that needs to specifically include the Bundestag. Based on a strong domestic performance, Germany could become a catalyst for global action: utilizing its diplomatic relations with countries from the Global South, Germany could advocate for investing in resilient ICT infrastructures, provide necessary CCB measures in partner countries, and support the strengthening of multilateral efforts.

Acronyms

CCB	Cybersecurity capacity building
CMM	Cybersecurity Capacity Maturity Model
CRI	Cyber Readiness Index
CSIRT	Computer Security Incident Response Team
EU	European Union
FIRST	Forum for Incident Response and Security Teams
G20	Group of Twenty
GCSCC	Global Cyber Security Capacity Centre
GFCE	Global Forum of Cyber Expertise
GLACY	Global Action on Cybercrime
ICT	Information and communication technology
ICT4D	Information and communication technology for development
IT	Information technology
ITU	International Telecommunications Union
NCSC	National Cyber Security Centre
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
UK	United Kingdom
UN	United Nations
UNDP	United Nations Development Programme
UNODC	United Nations Office on Drugs and Crime
US	United States
ZIF	Zentrum für Internationale Friedenseinsätze (Center for International Peace Operations)

Introduction

Information and communication technologies (ICTs) have been a boon for development and growth. In the G20 countries alone, the collective digital economy was estimated to be worth $4 trillion in 2016 and is growing at 10 percent per year.[1] An even larger potential exists in countries with developing economies, which are home to most of the one billion people expected to go online by 2020.[2] ICTs not only contribute to the (digital) economy, but also impact the progress of other parts of our societies, such as education, energy, or health. As a result, they have become critical catalysts for achieving the Sustainable Development Goals as defined in the 2030 Agenda for Sustainable Development.[3]

At the same time, it has become clear that no country will be able to reap the full potential of ICTs if they do not address the risks associated with connectivity. Data breaches, cybercrime, and attacks on critical infrastructure are increasing in scale and severity, and are unlikely to ebb anytime soon.[4] According to one estimate, cybercrime alone could cost the global economy over $500 billion a year.[5] While such estimates should be treated with caution, there is no doubt that the potential dangers related to cybercrime and insecure infrastructures affect public and private organizations, as well as individuals. Moreover, these threats undermine trust in online activities, which is fundamental for ICTs to have the greatest economic and societal impact.[6]

While no country is "cyber ready,"[7] nations with less developed IT infrastructures – which are expanding connectivity at four times the rate of developed countries – face

1 *Expanding Participation and Boosting Growth: The Infrastructure Needs of the Digital Economy*. World Economic Forum, 2015: 7. Last accessed on January 2, 2017. http://www3.weforum.org/docs/WEFUSA_DigitalInfrastructure_Report2015.pdf.

2 According to the ITU, the 49% of the world's households have internet access at home. This number, however, drops to 37.6% in developoing countries, and is at 81.3% in developed countries. International Telecommunication Union, ICT Facts and Figures 2016."

3 International Telecommunication Union, "ICTs for a Sustainable World #ICT4SDG," http://www.itu.int/en/sustainable-world/Pages/default.aspx, last accessed on January 2, 2017.

4 Johannes M. Bauer and William H. Dutton, *The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet*. World Bank, 2015. Last accessed on December 12, 2016. https://openknowledge.worldbank.org/bitstream/handle/10986/23641/WDR16-BP-The-New-Cybersecurity-Agenda-Bauer-Dutton.pdf;sequence=1.

5 *Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Report Summary*. Center for Strategic and International Studies, 2014: 2. Last accessed on January 2, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf.

6 Maria Grazia Porcedda, "Rule of Law and Human Rights in Cyberspace," in *Riding the digital wave: the impact of cyber capacity building on human development*, ed. Patryk Pawlak (European Union Institute for Security Studies, 2014): 28. Last accessed on January 5, 2017. http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf.

7 Melissa Hathaway et al., *Cyber Readiness Index 2.0*. Potomac Institute for Policy Studies, 2015. Last accessed on December 21, 2016. http://www.potomacinstitute.org/images/CRIndex2.0.pdf

particular challenges.[8] At this rapid pace, security often remains an afterthought. Research shows that, for example, malicious software is more prevalent within nations that are beginning to expand the use of information and communications technologies, but might be "unprepared to secure their ICT infrastructure commensurate with the increase in citizen use of computer systems."[9] As a recent alleged denial of service attack on Liberia's national internet network demonstrates, there are real concerns that attacks have the potential to take entire countries offline.[10]

Cybersecurity, then, is essential. As a means to ensuring resilient digital infrastructures, cybersecurity is crucial for countries to reap the the full economic and social benefits of ICT-led growth.[11] Recognizing this, governments and international organizations have put greater emphasis on cybersecurity in the global political and security agenda, as well as the broader development agenda. For example, in its 2016 report on "digital dividends" – i.e., the potential gains from investments into digital technologies – the World Bank stresses that cybersecurity poses a "significant problem" since the lack thereof affects public confidence and trust in online systems.[12] The International Telecommunications Union (ITU) calls it "one of the most profound challenges of our time,"[13] while the Organisation for Economic Co-operation and Development (OECD) calls for cooperation on the issue "across borders at regional and international levels."[14]

These challenges have led organizations such as the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security to stress the "vital importance" of cybersecurity capacity building (CCB) as a means to "bridge the divide in the security of ICTs and their use."[15] In parallel to building international norms for cyberspace and enhancing confidence-building measures, CCB has become a key pillar in global efforts to "reduce

8 United Nations News Centre, "Internet well on way to 3 billion users, UN telecom agency reports," (5 May, 2014), http://www.un.org/apps/news/story.asp?NewsID=47729#.WE504iQkyUl, last accessed on December 12, 2016.

9 David Burt et al., *The Cybersecurity Risk Paradox: Measuring the Impact of Social, Economic, and Technological Factors on Rates of Malware*. Microsoft Security Intelligence Report, 2014: 8. Last accessed on January 2, 2017. https://blogs.microsoft.com/microsoftsecure/2014/01/16/the-cybersecurity-risk-paradox-measuring-the-impact-of-social-economic-and-technological-factors-on-cybersecurity/.

10 Brian Krebs, "Did the Mirai Botnet Really Take Liberia Offline?," *KrebsOnSecurity* (Novermber 4, 2016), https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-really-take-liberia-offline/, last accessed on January 2, 2017.

11 Alexander Klimburg and Hugo Zylberberg, *Cyber Security Capacity Building: Developing Access*. Norwegian Institute of International Affairs, 2015. Last accessed on December 21, 2016. https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf.

12 *Digital Dividends, Flagship Report*. World Bank, 2016. Last accessed on December 21, 2016. http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.

13 Stein Schjølberg, *Report of the Chairman of HLEG*. ITU Global Cybersecurity Agenda (GCA), 2008. Last accessed on December 12, 2016. http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf.

14 *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*. Organisation for Economic Co-operation and Development, 2015. Last accessed on December 12, 2016. http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=328&InstrumentPID=371&Lang=en&Book=False.

15 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations General Assembly, 2015. Last accessed on December 12, 2016. https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf.

risk and enhance security [and to] promote a peaceful, secure, open, and cooperative ICT environment."[16]

In addition to unlocking the full economic and societal potential of ICTs, especially for the Global South, two factors drive the increasing attention to CCB in more technologically advanced countries. First, there is the desire to protect against the spread of negative cross-border externalities of vulnerabilities. In a globally connected digital system, vulnerabilities in one country are also a threat to other nations. Without effective law enforcement capacities, safe havens for cybercrime can arise, and insecure technical systems in one place can be abused to disrupt infrastructures somewhere around the globe. With not only more users, but more devices going online (as part of the Internet of Things), these cross-border problems are only set to increase and provide an incentive for all countries to increase the resilience of systems where they still are weakest. Second, CCB is increasingly seen as a tool of foreign policy.[17] Efforts to build capacity can also serve to advocate for a particular model of internet governance. At the same time, a government's projects can create market access for domestic companies and promote specific technical standards.

As a result of the different factors mentioned above, a community of professionals is emerging in foreign ministries, development agencies, international organizations, the private sector, and research institutes. With expertise in IT, security, or development, these professionals are dedicating themselves to closing the cybersecurity capacity gap. They are carrying out trainings and workshops for law enforcement officers, supporting the development of legislative frameworks or national cybersecurity strategies, helping to establish Computer Security Incident Response Teams (CSIRTs), or implementing awareness-raising campaigns for individuals, just to cite a few examples.

Despite their work, the present supply falls short of what is needed to transform cybersecurity from an afterthought into an integral part of expanding connectivity. Moreover, present efforts are often uncoordinated, not only internationally but also domestically, and there is little systematic exchange, let alone integration, between cybersecurity and development actors as well as diplomats. Awareness of capacity building pitfalls that have plagued efforts in other areas is growing, but slowly. Additionally, funding is limited, and as a result the number of past and present cybersecurity capacity building projects is small, offering few models for best practices, let alone lessons learned or thorough evaluations. As a general challenge, all governments involved are struggling to build up as well as retain the technical expertise that is critical for successful CCB, and public-private cooperation remains limited. While a few governments, like the Netherlands, the UK and the United States, have invested resources into CCB, in most countries as well as international organizations and corporations, the topic lacks the sustained top-level leadership attention and support that will be essential if CCB is to live up to its potential by scaling up and professionalizing.

---

16 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations General Assembly, 2013: 2. Last accessed on December 21, 2016. https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf.

17 Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy."

On the upside, CCB provides a political opportunity with promising returns on investments. As we outline in part two, a few pioneers have already done a lot of work, which could be scaled with increasing political attention and funding. In part three, we aim to contribute to charting a path that shows how policymakers can advance CCB. To this end, we develop a principle-based approach to analyze how the status quo falls short of the goals of CCB and offer recommendations on how to close this gap. Finally, we present two scenarios to show divergent possible futures for cybersecurity capacity, and draw conclusions as to how a country such as Germany could contribute to advancing CCB on both the domestic and international level.

Cybersecurity Capacity Building: An Overview

Definition and Scope

Most frameworks understand capacity building[18] as initiatives to strengthen existing in-country capacities that help individuals, organizations, or social systems achieve their development goals.[19,20] This understanding is reflected in the definition of cybersecurity capacity building that we adopt in this study: "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."[21,22] This definition recognizes that cybersecurity capacity building is key to managing risks that are technical in nature but that broadly affect economies and societies, for example by limiting growth that could be attained by the adoption of ICTs, or by degrading individuals' privacy if insecure systems lead to data leaks.

This definition stresses the importance of building resilient systems – that is, systems that are able to "withstand and recover from deliberate attacks, accidents,

18 While recognizing the contextual existence of capacities prior to endogenous development efforts, this study employs the term capacity building, and not the term capacity development. This is owed to the almost unilateral use of the term in cybersecurity capacity building literature and our goal of contributing to the harmonization rather than fragmentation of the field.

19 The German development organization GTZ (now GIZ) identifies institutional and legal capacity, organizational capacity and human resource capacity as three key areas of intervention. Ilka N. Buss, *Best Practices in Capacity Building Approaches*. Deutsche Gesellschaft für Technische Zusammenarbeit, 2010. Last accessed on December 21, 2016. http://ledsgp.org/wp-content/uploads/2015/07/Best-Practices-in-Capacity-Building-Approaches.pdf.

20 Hettie Walters, *Capacity Development, Institutional Change and Theory of Change: What do we mean and where are the linkages* Wageningen International, 2007. Last accessed on December 12, 2016. http://portals.wi.wur.nl/files/docs/successfailuredevelopment/Walters_CapacityDevelopmentConceptPaperFIN.pdf. Joe Bolger, *Capacity Development: Why, What and How*. Canadian International Development Agency, 2000. Last accessed on December 9, 2016. http://www.hiproweb.org/fileadmin/cdroms/Biblio_Renforcement/documents/Chapter-1/Chap1Doc1.pdf.

21 This is based on the definition of cybersecurity that is put forward in: Patryk Pawlak, *Riding the digital wave: the impact of cyber capacity building on human development*. European Union Institute for Security Studies, 2014: Introduction. Last accessed on December 21, 2016. http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf.

22 "Digital security risk... is the expression used to describe a category of risk related to the use, development and management of the digital environment in the course of any activity. This risk can result from the combination of threats and vulnerabilities in the digital environment" in *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*. Organisation for Economic Co-operation and Development: 10.

or naturally occurring threats or incidents."[23] Just as cybersecurity is not the sole responsibility of governments, cybersecurity capacity building should not be framed as a soley intergovernmental issue, but rather one that requires a multi-stakeholder approach – nationally and across various jurisdictions.

In line with such a comprehensive approach, CCB efforts cover a broad set of activities. The Global Cyber Security Capacity Centre's (GCSCC) National Cybersecurity Capacity Maturity Model (CMM; see figure 1) provides a useful overview and framework for understanding national cybersecurity capacity. The CMM's five dimensions and the various sub-categories (factors) illustrate that raising awareness is just as much part of cybersecurity capacity building as creating legal frameworks or enhancing technical expertise.

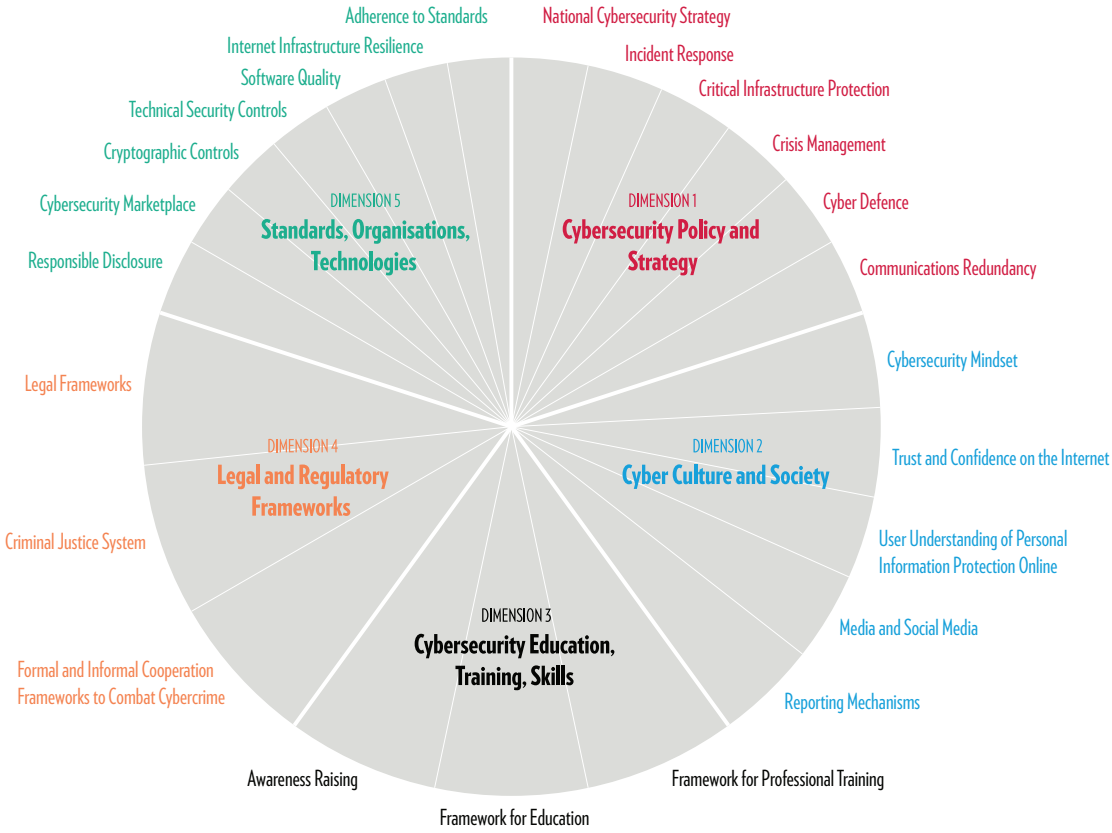

Figure: Categories of the National Cybersecurity Capacity Maturity Model[24]

23 Department of Homeland Security, "What Is Security and Resilience?" https://www.dhs.gov/what-security-and-resilience, last accessed on January 2, 2017.

24 Based on: Global Cyber Security Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition" (February 9, 2017), https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf, last accessed on February 25, 2017.

The model requires political judgment-calls. If cybersecurity is understood to be more than a technical challenge, different normative understandings of what should be achieved through capacity building efforts emerge. For countries or organizations that provide capacity building services, this means deciding which exact services (not) to provide in the countries where they carry out projects. Given that some of these measures aim to increase the operational capabilities of states, there is an inherent challenge posed by the dual-use nature of many cybersecurity skills and techniques. Just as security assistance programs have enabled human rights abuses (for example, by training and equipping abusive security forces), cybersecurity capacities could also be used for malicious purposes. Potential for abuse needs to be taken into account when deciding whom to work with and how to monitor CCB efforts. When doing so, it is also important to keep in mind that authoritarian actors, which espouse a very different set of values and policies, are also going to increase their cybersecurity capacity building efforts. Therefore, Western efforts should be risk-aware but not totally risk-averse, since this would mean leaving the CCB field open to actors who may deliver on a full-fledged agenda of surveillance and social control with their CCB offerings.

Actors and Activities

A variety of governments, regional and international organizations, as well as non-state actors have been carrying out activities to increase cybersecurity capacity in several of the categories mentioned above. This section aims to provide a better idea of who relevant actors are, and what their activities look like.

National Governments

Although the responsibility for cybersecurity capacity building is shared by many stakeholders, governments often lead coordinating efforts. [25] Some of the most active Western countries include the Netherlands, the United Kingdom, and the United States. It is worthwhile to look at their CCB efforts to better understand the field.[26]

In its 2013 national cybersecurity strategy, the Netherlands stated that it seeks to "build coalitions for freedom, security and peace in the digital domain" and that it commits itself to expanding cybersecurity in third countries. In 2011, the US published an *International Strategy for Cyberspace*; the document outlined, among other objectives, the need to "provide the necessary knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity."[27] And according to its 2016 national cybersecurity strategy, the UK will "work to build the capacity of our

25 Patryk Pawlak, *Cyber Capacity Building in Ten Points*. European Union Institute for Security Studies, 2014: 12. Last accessed on December 9, 2016. http://www.iss.europa.eu/uploads/media/EUISS_Conference-Capacity_building_in_ten_points-0414.pdf.

26 Other active countries include Israel, South Korea and Japan. The Netherlands, UK, and US were selected for closer analysis, since their overall national setup and diplomatic activities resemble more closely that of Germany and because there was more public data available.

27 *International Strategy for Cyberspace*. The White House, 2011: 22. Last accessed on January 6, 2016. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

partners to improve their own cyber security," acknowledging that it also does so "in order to reduce the threat to the UK and our interests."[28]

In addition to raising awareness of CCB in their cybersecurity strategies, all three countries have attempted to streamline their efforts and responsibilities and assign clear responsibilities domestically. In the Netherlands, the National Cyber Security Centre (NCSC) was created to coordinate the work of various bodies tasked with aspects related to cybersecurity, including capacity building.[29] The NCSC is part of the Cyber Security Department, which is overseen by the Dutch Ministry of Security and Justice. In the UK, the Foreign and Commonwealth Office manages the International Cyber Security Capacity Building Programme, which aims to bolster cyber capacity building abroad.[30] In the US, the State Department "leads the government's diplomatic and development engagement on activities in cyberspace,"[31] and within the department, the Office of the Coordinator for Cyber Issues is also in charge of cybersecurity capacity building.[32]

The Netherlands, the UK, and the US have carried out a variety of activities in the field of cybersecurity capacity building.[33] Of the three, the UK has implemented the widest range of projects. It has conduced training programs for CSIRTs, supported CyberGreen (an initiative to "improve the health of the global Cyber Ecosystem"[34]), and, most notably, provided seed-funding and continued support for the Martin School's Global Cyber Security Capacity Centre (GCSCC) at Oxford University.[35] In the US, the Office of the Coordinator for Cyber has overseen the successful implementation of several projects, such as workshops for officials from sub-Saharan African nations on tackling cybercrime, or the launch of a global awareness campaign on cybersecurity.[36] The Netherlands, meanwhile, has been particularly active in launching international initiatives. After hosting the Global Conference on Cyberspace in 2015, the Netherlands

---

28 *National Cyber Security Strategy 2016-2021*. Government of the United Kingdom, 2016: 61. Last accessed on January 3, 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

29 The National Cyber Security Centre, "What is the NCSC?," https://www.ncsc.nl/english/organisation, last accessed on January 2, 2017.

30 Government of the United Kingdom, "FCO Cyber Security Capacity Building Programme 2017 to 2018," https://www.gov.uk/government/publications/fco-cyber-security-capacity-building-programme-2017-to-2018, last accessed on January 3, 2017.

31 *Department of State International Cyberspace Policy Strategy*. U.S. State Department of State, 2016: 1. Last accessed on January 3, 2017. https://www.state.gov/documents/organization/255732.pdf.

32 Piret Pernik, Jesse Wojtkowiak, and Alexander Verschoor-Kirss, *National Cyber Security Organisation: UNITED STATES*. NATO Cooperative Cyber Defence Centre of Excellence, 2016: 15. Last accessed on January 2, 2017. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf.

33 To provide a better insight into some of the projects that have been carried out in the past, four projects are presented in greater detail in the Annex.

34 Global Forum on Cyber Expertise, "CyberGreen," https://www.thegfce.com/initiatives/c/cybergreen, last accessed on January 3, 2017.

35 Government of the United Kingdom, "Oxford will host Cyber Security Capacity Building Centre," (April 9, 2013), https://www.gov.uk/government/news/oxford-will-host-cyber-security-capacity-building-centre, last accessed on January 3, 2017.

36 USDepartment of State, "Office of the Coordinator for Cyber Issues," https://www.state.gov/s/cyberissues/, last accessed on January 2, 2017. Global Forum on Cyber Expertise, "Promoting Cybersecurity Due Diligence across Africa," https://www.thegfce.com/initiatives/p/promoting-cybersecurity-due-diligence-across-africa, last accessed on January 2,2017. Global Forum on Cyber Expertise, "Global Campaign to Raise Cybersecurity Awareness," https://www.thegfce.com/initiatives/g/global-campaign-to-raise-cybersecurity-awareness, last accessed on January 2, 2017.

co-initiated the Global Forum on Cyber Expertise (GFCE). The Dutch government has also been actively involved in the Internet Infrastructure Initiative to build robust infrastructures abroad, and the Coordinated Vulnerability Disclosure Initiative, a platform to exchange experiences and lessons learned in disclosing software and hardware vulnerabilities.[37]

Regional and International Organizations

In addition to the initiatives of individual states, regional and international organizations have substantially contributed to cybersecurity capacity building. For instance, a joint project by the Council of Europe and the European Union, based on the Budapest Convention on Cybercrime, aims to support criminal justice authorities worldwide to combat cybercrime,[38] and various experts have praised this project as comprehensive and successful. In its cybersecurity strategy, the European Union points out that it "will actively participate in international efforts to build cybersecurity capacity," and through its Instrument contributing to Stability and Peace, the EU committed about €21.5 million for CCB and fighting cybercrime in the period from 2014 to 2017.[39] As another example of successful cooperation, the Organization of American States has supported its member states in establishing CSIRTs, drafting cybersecurity strategies and monitoring cybercrime for over a decade.[40]

On the global level, cybersecurity capacity building is part of the mandate of the International Telecommunications Union (ITU), the United Nations' specialized agency responsible for ICTs.[41] While sometimes perceived as too state-centric and therefore in conflict with the multi-stakeholder approach generally favored by Western countries, the ITU conducts a number of projects, ranging from those that support the establishment of harmonized ICT policies to those that conduct cyber drills in different regions of the world.[42] Another UN agency, the United Nations Development Programme (UNDP), has recognized the issue as a challenge, but has yet to provide

37 Global Forum on Cyber Expertise, "CSIRT Maturity Initiative," https://www.thegfce.com/initiatives/c/csirt-maturity-initiative, last accessed on January 2, 2017. Global Forum on Cyber Expertise, "Coordinated Vulnerability Disclosure," https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking last accessed on January 2, 2017.

38 Council of Europe, "Global Action on Cybercrime," http://www.coe.int/en/web/cybercrime/glacy, last accessed on January 2, 2017.

39 *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* European Commission, 2013: 15. Last accessed on January 5, 2016. http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. Pawlak, *Riding the digital wave: the impact of cyber capacity building on human development*. European Union Institute for Security Studies: Introduction, 5.

40 Organization of American States, "Cyber Security," https://www.sites.oas.org/cyber/en/pages/default.aspx, last accessed on January 3, 2017.

41 International Telecommunication Union, "About ITU," http://www.itu.int/en/about/Pages/default.aspx, last accessed on January 2, 2017.

42 International Telecommunication Union, "ITU-EC-ACP Project," http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx, last accessed on January 2, 2017. *ITU-Impact, Applied Learning for Emergency Response Teams (ALERT)*. International Telecommunication Union, 2013. Last accessed on January 2, 2017. https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/ITU-IMPACT%20ALERT.pdf. Patryk Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy," *Global Policy* 7, no. 1 (2016): 89.

many services.[43] The United Nations Office on Drugs and Crime (UNODC) is supporting nations in understanding their needs to fight cybercrime and is carrying out trainings with law enforcement agencies, for example on cybercrime investigations and digital forensics.[44]

To increase international coordination among stakeholders, the Global Forum of Cyber Expertise was created in 2015. Its aim is to provide a "pragmatic, action-oriented and flexible forum" to all relevant stakeholders with the resources to contribute to cybersecurity capacity building.[45] To date, members include countries, international organizations, and companies who convene annual, high-level meetings, among other activities. To facilitate the exchange of information, information on projects by GFCE members is published online.[46]

Non-State Actors

Non-state actors – including technical and non-profit organizations, research institutions, and the private sector – play a vital role in cybersecurity capacity building. Technical organizations, such as the Forum on Incident Response and Security Teams, have a track record of supporting the establishment, growth, and networking of new Computer Security Incident Response Teams. Not-for-profit organizations, such as ICT4Peace, Clingendael and Global Partners Digital, have also carried out projects, often raising awareness or helping individuals improve their cybersecurity expertise.

Several research institutions and universities work on cybersecurity capacity building as well. So far, their most prominent contribution has been the development of a number of cyber maturity models, such as the Potomac Institute's Cyber Readiness Index (CRI) 2.0 and Oxford's CMM.[47] These allow a country to assess and benchmark their cybersecurity capacity maturity, enabling policymakers to define priorities going forward. In addition, workshops with various national statekholders, which, for example, the CMM is carrying out, provide a useful starting point for a first discussion on potential CCB efforts. The GCSCC at Oxford also manages the Cybersecurity Capacity Portal, a publicly-available online resource which publicizes CCB knowledge, provides an inventory of international and regional initiatives, and offers an overview of relevant events.[48]

---

43 Paul Raines, "UNDP Cybersecurity Assistance for Developing Nations," *CSO50 Confab* (April 18, 2016), http://www.csoconfab.com/wp-content/uploads/2016/03/CSO50_2016_Paul-Raines_Providing-Effective-Cybersecurity.pdf, last accessed on January 2, 2017.

44 *UNODC Annual Report 2015*. United Nations Office on Drugs and Crime, 2015: 57, 58. Last accessed on January 5, 2017. http://www.unodc.org/documents/AnnualReport2015/Annual_Report_2016_WEB.pdf.

45 *The Hague Declaration on the GFCE*. Global Forum on Cyber Expertise, 2015: 1. Last accessed on January 2, 2017. https://www.thegfce.com/about/documents/publications/2015/04/16/the-hague-declaration-on-the-gfce.

46 Global Forum on Cyber Expertise, "Initiatives," https://www.thegfce.com/initiatives, last accessed on January 2, 2017.

47 Hathaway et al., *Cyber Readiness Index 2.0*. Potomac Institute for Policy Studies.; Global Cyber Security Capacity Centre, "Cybersecurity Capacity of the UK." For more information on the two models, please consult Annex 2.

48 Global Cyber Security Capacity Centre, "A Global Resource for Cybersecurity Capacity Building," https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front, last accessed on January 3, 2017.

Finally, the private sector's role cannot be stressed enough. Given that most IT infrastructures are in private hands, many companies in recipient countries are already providing important security functions, and international technology companies have long been driving cybersecurity innovation.[49] With regards to (state-led) CCB efforts, however, companies have yet to be integrated more, even though some have become involved in individual projects. For instance, Hewlett Packard supports the Vulnerability Disclosure Initiative, while Microsoft supports the ITU's National Cybersecurity Strategies project, among others.[50] In addition, various other large technology companies, such as Symantec, IBM, and Huawei, are members of the GFCE and support and carry out different projects.[51]

49 Niels Nagelhus Schia, *'Teach a person how to surf': Cyber security as development assistance*. Norwegian Institute of International Affairs, 2016: 26. Last accessed on January 5, 2017. https://brage.bibsys.no/xmlui/bitstream/id/415569/NUPI_Report_4_16_Nagelhus_Schia.pdf.

50 Global Forum on Cyber Expertise, "Coordinated Vulnerability Disclosure." International Telecommunications Union, "National Strategies," http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx, last accessed on January 19, 2017.

51 Global Forum on Cyber Expertise, "Overview Members," https://www.thegfce.com/organization/members/overview-members, last accessed on January 2, 2017.

Towards a Principle-Based Approach: Goals, Status Quo, Recommendations

As the last section has shown, activities in the field of cybersecurity capacity building (CCB) have increased over the last few years, and the uptake in conferences and literature on the issue suggests that more actors are expanding their work on the issue. These developments should be welcomed. Still, the number of projects remains limited and a lack of coordination risks wasting resources through duplication. In addition, closer attention needs to be paid to how current activities are being carried out, so that best practices can be scaled successfully. To assess current gaps and provide a direction for a concerted, effective effort moving forward, we developed the following five guiding principles:

- National and international coordination and cooperation;
- Integration of cybersecurity and development expertise;
- Ownership of the recipient-country;
- Sustainability of efforts;
- Continued and mutual learning.

These principles are based on the interviews we conducted with over 40 experts in the field, as well as a broad literature review. For each of the them, we suggest a goal – i.e. an ideal set-up –, analyze the status quo, and provide recommendations on how to work towards the goal. Recognizing that there is no need to "reinvent the wheel" in capacity building, the principles point – where appropriate – to lessons learned from other areas of capacity building.

Coordination and Cooperation

National Coordination and Cooperation

Goal: For countries willing to invest in the field, the aim should be to effectively fund, design, and deliver CCB measures. To this end, all relevant stakeholders, especially in government, but also civil society and the private sector, need to coordinate their activities and, to the degree possible, cooperate in carrying out measures.

Status quo: Most donor countries have only taken a piecemeal approach to CCB coordination so far, if they are aware of the issue at all. Since it is still a fairly new and in the eyes of many obscure topic, government bodies tasked with CCB often have unclear mandates. Frequently, there is little funding available for such projects. In addition, due to the many different aspects of CCB, different units within an administration are often partially responsible and at times in competition with each other. As a result, the issue is often not dealt with. Moreover, despite the increasing need in and demand from recipient countries, most donor countries have a clear policy neither on how to best prioritize CCB measures nor on how to pick suitable partner countries. Only a few countries have already installed coordinating agencies (e.g., the UK's International Cyber Security Capacity Building Programme).

Cooperation between governments and other national stakeholders often remains limited. While companies also have an interest in secure infrastructures (and potentially expanding their market access), there are few tangible incentives to participate in or sponsor (state-led) CCB programs. Even for many IT companies these issues are not seen as key corporate social responsibility efforts, despite the fact that CCB would fit the bill very well. In general, lack of experienced staff is a problem: Governments around the globe are currently seeking more IT experts and might be unable or unwilling to use those resources abroad.

Recommendations

Develop a national CCB approach and prioritize. The strategy process should involve the different key actors from government (including diplomacy, security, and development), as well as important corporate, academic and non-profit players. In order to pursue a coherent approach to CCB, a precise understanding of cybersecurity is a crucial starting point. Therefore, building on a national cybersecurity strategy can be useful, as long as it is recognized that capacity building abroad will only indirectly contribute to one's own security. Based on this approach, natios can decide how to focus their efforts in accordance with their relative strengths, domestic experience, and interest – and which countries they want to coordinate with.

Streamline institutional setup. In line with the approach, roles and responsibilities around CCB should be clarified, including a decision on which office or person in the administration will coordinate all CCB efforts. Equipped with a clearly delineated mandate, the selected entity should coordinate CCB projects and integrate relevant stakeholders in the planning of CCB efforts – including foreign ministries, development agencies, national information security agencies, civil society, academia, and the private sector.

Make use of maturity models and indices. Given the broad spectrum of CCB activities, existing frameworks such as the Cybersecurity Capacity Maturity Model (CMM) can provide guidance when conceptualizing the different areas of cybersecurity capacity building and when making decisions on which capacities to invest in. More importantly, maturity models that assess a country's cybersecurity readiness should be consulted in order to make informed decisions when selecting partner countries and developing programs.

Involve civil society and the private sector in projects. Experts largely agree that the involvement of the private sector and civil society in planning and implementing CCB initiatives is crucial, as they can provide input on technical questions, but also potentially act as contracting partners if governments lack the staff to carry out projects. Companies in the IT sector could also integrate CCB into their corporate social responsibility activities, and governments should attempt to mobilize the private sector, for example by actively involving them in a very relevant challenge that needs to be solved cooperatively.

Build a CCB capacity pool. Mirrored on schemes in other areas (e.g., election monitoring or civilian crisis management as coordinated in Germany by the Center for International Peace Operations, or ZIF), governments should draw up a roster of experts who are willing and qualified to engage in CCB. This should include individuals from government and the private sector, as well as non-profits and research institutes.

International Coordination and Cooperation

Goal: On the international level, limited resources should be maximized by avoiding duplication of CCB efforts. This requires increasing coordination and knowledge sharing among donors, as well as cooperation on specific projects.

Status quo: As outlined in section two, various actors are active in the field, but they have no concerted approach to follow, and there is little structured communication on respective efforts. Most communication happens only ad hoc and often informally, leading one expert to claim that "right now, it's a mess."[52] Many countries or organizations do not make their efforts public, thus it is a "consistent challenge" to gain an overview on current projects and to locate actors that are working on the same topic.[53] While organizations such as the EU and the Organization of American States (OAS) have begun to coordinate regional efforts, there is little international communication, leading to duplication of efforts – for example, workshops with similar stakeholders taking place in parallel, just shortly after one another.[54] While many individuals involved have a good understanding of initiatives in the field, this is often true because the community is still fairly small – and is unlikely to hold if efforts were significantly expanded.

The first attempt to set up coordination on the global level was the establishment of the GFCE as an international platform for CCB stakeholders. The GFCE is a step in the right direction, but at this point serves mostly as a repository for various initiatives. It remains to be seen whether its members will be able to shape the GFCE into an efficient coordinating body. The GFCE and Oxford's GCSCC are also cooperating on the Cybersecurity Capacity Portal, an online repository of past and present CCB initiatives,

52 Interview conducted on October 24, 2016.

53 Lilly Pijnenburg Muller, *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*. 2015: 16. Last accessed on December 9, 2016. https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf.

54 Interview conducted on October 11, 2016; Patryk Pawlak, "Developing Capacities in Cyberspace," in *Riding the digital wave: the impact of cyber capacity building on human development*, ed. Patryk Pawlak (European Union Institute for Security Studies, 2015): 17. Last accessed on January 5, 2017. http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf.

events, and publications in order to overcome some of the aforementioned hurdles to cooperation.[55]

This state of affairs is further exacerbated by a lack of trust among states due in part to different views regarding cybersecurity. The GFCE, for example, envisions a "[f]ree, open and secure"[56] cyberspace – an outlook that is shared among most Western nations, but alienates key cybersecurity players, such as Russia and China, who both provide scant public information on their cybersecurity capacity building activities. The ITU is currently restructuring its cybersecurity efforts, and it remains to be seen what the new program will attempt to achieve and to what extent they will be recognized by a broad set of member states. In the past, critics have pointed out that the ITU, as a government-centric institution, takes a top-down approach and holds a problematic understanding of cybersecurity and internet governance that was promoted by individual member countries.[57]

Recommendations

Strengthen multilateral coordination and delineate mandates. Either bilaterally or through an international platform, coordination should be improved. As a platform, a number of options seem feasible. The GFCE could be developed into the main forum that shapes the global agenda on CCB. For that to happen, there needs to be more support for the forum, and more countries need to actively support the Dutch in their efforts. Alternatively, the ITU could expand the scope of its existing work in the field, yet under the condition that such an effort would be taken as part of a multi-stakeholder approach. In parallel, the G20, as the group of countries with major economic clout, is a suitable platform for coordination among key countries involved in providing CCB.

Communicate efforts and best practices. Donors should strive to jointly make the best use of their limited resources by avoiding duplication. This necessitates communication on CCB efforts though multilateral platforms like the GFCE or online portals. For example, Oxford's Cybersecurity Capacity Portal could be enhanced to provide a comprehensive and concise overview on efforts. To accelerate the learning process of donor and recipient countries alike, donors need to share best practices and actively promote lessons learned from past projects through these platforms. Instead of creating competition among donors, these efforts should focus on how each actor can contribute added value to CCB initiatives.

Make international cooperation inclusive and strengthen regional efforts. International coordination platforms should take into account the perspectives of donors and recipients alike. In addition, regional organizations such as the OAS, the African Union, or the OSCE should be supported in taking a more active role. Regional organizations can serve as multipliers and a means of strengthening South-to-South cooperation. Experience gained and lessons learned can be distributed via the information sharing platforms mentioned above.

---

55 More information can be found online at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front

56 Global Forum on Cyber Expertise, "Vision and ambition," https://www.thegfce.com/about/contents/vision, last accessed on January 2, 2017.

57 Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy," 89.

Integration

Goal: With cybersecurity playing an integral part in accomplishing development goals across sectors, actors especially from, but not limited to, the development and cybersecurity community should cooperate, or at the very least coordinate, on projects. Thinking about cybersecurity should be part of every measure that relates to ICT for development (ICT4D). Otherwise, increasing digitalization in the Global South bears risks, and putting 'safe locks' on ICT infrastructure from the beginning is less costly than mitigating damages later.

Status quo: The development community has only hesitantly begun to officially recognize cybersecurity as an important issue in the development field. Cybersecurity, or "resilience," is mentioned, but not prominently featured, in both the World Bank's World Development Report on Digital Dividends and the Bank's "Digital Development Partnership," which is meant to put the report into action.[58] Within the UNDP, there is the recognition that "cyberspace introduces new risks and vulnerabilities," but few explicit projects have been carried out so far.[59] Many large-scale ICT4D projects focus on increasing internet access in the Global South, but there is still little involvement of development agencies in CCB projects. This is unfortunate, as development agencies have valuable expertise in traditional capacity development, good knowledge of the political environment in the recipient countries, and often access to long-term funding. To explain this state of affairs, most experts point to development actors' uneasy relationship with cyber*security* capacity building. Often without the mandate to handle, or abundant experience in, traditional security issues, they are hesitant to become engaged.

In effect, the current digitalization, often fuelled by development funding, takes place without necessarily ensuring the resilience of systems. Moving forward, the technical expertise of cybersecurity professionals should ideally be integrated with the procedural experience on capacity building in the development community.

Recommendations

Break down the silos. The binary narrative, according to which the economy and security are two distinct aspects of cyberspace, needs to be critically questioned. An integrated approach should be advocated, with an emphasis on the mutual benefits that actors from the development and cybersecurity fields can gain through cooperation. Language plays a key role here: speaking of "digital risks" and "resilience" instead of "cybersecurity" can help demonstrate that capacity building strengthens not only national security but especially economic and social development. This does not

58 World Bank, "Digital Development Partnership," (June, 2016), http://cwi.unik.no/images/8/8c/DDP_partnership_brochure_draft22Jun2016.pdf, last accessed on January 2, 2017.

59 United Nations Development Programme Press Center, "'Seoul framework' could make cyberspace safer, more accessible," (October 18, 2013), http://www.undp.org/content/seoul_policy_center/en/home/presscenter/articles/2013/10/18/-seoul-framework-could-make-cyberspace-safer-more-accessible-.html, last accessed on January 2, 2017. Paul Raines, "Re-thinking development aid in the digital age," *CSO Online* (February 5, 2015), http://www.csoonline.com/article/2878566/cyber-attacks-espionage/re-thinking-development-aid-in-the-digital-age.html, last accessed on January 2, 2017.

prohibit a separation between projects that affect more traditional national security issues (such as training of law enforcement), and those that focus more directly on strengthening human rights (e.g., empowerment of individuals through awareness-raising);rather, it establishes that they both work towards a similar goal.

Make sure CCB projects are 'ODAble.' Linking cybersecurity capacity building efforts with the concept of Official Development Assistance as defined by the OECD Development Assistance Committee (DAC) would not only help integrate CCB measures into a recognized framework, but also increase the funding that is available for investment in the field.[60]

Increase number of joint projects. To strengthen cooperation, mutual understanding, and the quality of projects, there should be more projects that involve actors from the development community and the cybersecurity community. Experience gained and lessons learned can be distributed via the information sharing platform mentioned above.

Ownership

Goal: The willingness and interest of stakeholders in the recipient countries to engage and participate in CCB projects is a vital factor for their success, as capacity building often is ineffective if it is perceived as an exogenous measure.[61] Partner countries need to "exercise effective leadership over their development policies and strategies and co-ordinate development actions,"[62] including cybersecurity capacity building. It is crucial to ensure political buy-in from government officials and to directly engage with relevant actors who are willing to participate in CCB efforts in the. For CCB projects to be attractive, they have to be tailored to the needs of the respective recipient country; this cannot be done unless key players from recipient countries play a vital part in designing CCB measures.

Status quo: Experts point to discrepancies between donors' objectives and beneficiaries' priorities.[63] Recipients often have an interest in learning hands-on skills or receiving technical equipment, which donors are not always willing to provide. Donors also have their own political agendas and might be interested in promoting a certain model of internet governance or specific legal frameworks. Although these discrepancies will always exist to a certain degree, they should be taken into account when planning programs and when deciding which countries to cooperate with.

An additional challenge is that, when compared to the prevailing socio-economic problems in the Global South (and elsewhere), cybersecurity often looks less imminent. Thus, experts report a lack of willingness to take the lead regarding CCB measures

60 Klimburg and Zylberberg, *Cyber Security Capacity Building: Developing Access*. Norwegian Institute of International Affairs: 41.

61 *The Challenge of Capacity Development: Working Towards Good Practice*. Organisation for Economic Co-operation and Development, 2006. Last accessed on December 21, 2016. http://www.fao.org/fileadmin/templates/capacitybuilding/pdf/DAC_paper_final.pdf.

62 *The Paris Declaration on Aid Effectiveness*. Organisation for Economic Co-operation and Development, 2005: 5. Last accessed on January 2, 2017. https://www.oecd.org/dac/effectiveness/34428351.pdf.

63 Pawlak, *Cyber Capacity Building in Ten Points*. European Union Institute for Security Studies: 2.

among elites in the receiving countries. At the same time, some point out that "the demand is endless," and that there is a "cry for help" from a variety of countries.[64] Similarly, in a 2013 report of the United Nations Office on Drugs and Crime, "75 per cent of responding countries, across all regions of the world, reported requiring technical assistance in the area of cybercrime," with 100 percent of African nations doing so.[65]

Finally, civil servants in some countries, often overwhelmed with work on the ground, are more inclined to participate in short-term trainings than to become seriously engaged over the long term.

Recommendations

Recipient countries must develop their own strategies. Working with recipient countries to set their own strategic priorities gives a stronger impetus to commit to the successful delivery of CCB projects, and ensures interest and willingness to engage on this front by actors in the receiving countries. To avoid duplications, cybersecurity efforts could be laid out in national development plans or frameworks where such exist.

Ensure high-level institutional backing. With political support for CCB measures from domestic governments crucial to their effectiveness, it is necessary to develop the trust of high-level policymakers, also in recipient countries. In addition, before beginning closer cooperation, countries should have already demonstrated that they are committed to taking cybersecurity efforts seriously and that they recognize their responsibilities moving forward.

Base projects on prior capacity assessment. In order to fit a project to the actual needs of a recipient country, a prior capacity assessment – together with actors on the ground – should be used to determine the state of the partner country's existing capacities. To this end, maturity models such as Oxford's CMM or the Potomac Institute's CRI 2.0 may be helpful both to assess capacity and bring relevant national stakeholders together. However, while such models serve to assess capacity, they are "are just the first step, they're not capacity *building*."[66]

Sustainability

Goal: Capacity building is not a quick fix for isolated problems, but a long-term endeavor to address structural shortcomings in a sustainable manner. This also holds true for cybersecurity efforts, which will pay off especially if they are sustainable over time. This requires the creation of conditions in which countries acquire enough capacity to protect themselves from cyber threats in the future, especially since the threat landscape is evolving quickly. Accordingly, capacity building should not aim at providing training to an individual or a small group, but at integrating all relevant

64 Interviews conducted on October 18 and October 11, 2016.

65 *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime, 2013: 178. Last accessed on January 5, 2017. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

66 Interview conducted on September 28, 2016

stakeholders "that can have an influence on the performance of specific [capacity building] activities."[67]

Status quo: Since CCB has only recently gotten more traction, there is little knowledge – especially from the recipient countries' side – on what measures and programs work. While there are many short-term and one-off efforts in the form of workshops and trainings, only a few projects had a sufficiently large scale for putting sustainable structures in place. Yet such one-off trainings, while helping to raise some awareness, are limited in what they can achieve; one expert went as far as to argue that they are "useless – full stop."[68]

The difficulty of retaining qualified local experts (in the public sector) for a long-term commitment also hinders the retention of expertise. Tapping into much-needed private sector human resources has proven difficult, given the public-private salary discrepancy.

Recommendations

Define "who" needs "what" capacity for "what purpose."[69] This definition is important to keep in mind when deciding on what measures to provide. More broadly, any project must define goals, vision, strategy, and relevant concepts, all of which should be linked to the assessment of existing capacities and an actor analysis.[70]

Do not start from scratch. Experts agree that measures are likely to achieve more sustainable outcomes if they are based on already existing capacities in the recipient country. Rather than creating parallel structures, new projects should build on prior structures as much as possible.

Build on established methods and instruments. Again, learning from other areas of capacity building, donors can look to a range of activities that have proven useful in the past. Those include the concept of "training the trainers" – focusing on the training of local individuals or organizations that may then go on to train multipliers themselves, twinning – the pairing of each one local 'apprentice' and one external expert or practitioner – and the establishment of local technology centers.[71] While one-time events such as workshops or capacity assessments provide a starting point, they should not substitute for more complex projects focused on achieving long-term, tangible results. For efforts to be sustainable, there must be specific efforts that aim to increase the pool of experts in recipient countries.

---

67 Buss, *Best Practices in Capacity Building Approaches*. Deutsche Gesellschaft für Technische Zusammenarbeit: 10.

68 Email exchange wich expert on September 1, 2016

69 *Basics of Capacity Development for Disaster Risk Reduction*. CaDRI - Capacity for Disaster Reduction Initiative, 2012: 9-10. Last accessed on January 2, 2017. http://www.undp.org/content/undp/en/home/librarypage/crisis-prevention-and-recovery/basics-of-capacity-development-for-disaster-risk-reduction-.html.

70 Buss, *Best Practices in Capacity Building Approaches*. Deutsche Gesellschaft für Technische Zusammenarbeit: 12. Muller, *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*. 11.

71 Buss, *Best Practices in Capacity Building Approaches*. Deutsche Gesellschaft für Technische Zusammenarbeit: 17 pp.

Utilize a cross-sectoral approach. Where possible, civil society, the private sector, and academia should be involved in countries where CCB projects are being carried out, since the retention of expertise though government officials only can be challenging. Universities could help establish centers of excellence, and public-private partnerships could not only help to fund projects, but spread knowledge. As for private-sector involvement, it is important to not only involve large technology companies when devising or carrying CCB programs, but also the many small and medium enterprises that rely on cybersecurity, and can also be multipliers in recipient countries.[72]

Learning

Goal: An understanding of which measures have or have not worked and why can be of tremendous advantage in the conceptualization, implementation, and continued improvement of projects. To encourage continuous learning for all actors involved, frequent, structured, and thorough evaluation and feedback mechanisms are key instruments in the building of sustainable capacity. These mechanisms can help improve ongoing projects and enable better informed choices regarding future projects.

Status quo: The current challenges are threefold: First, there is not a clear consensus yet on which capacity measures work specifically in this field.[73] After all, "cybersecurity is new" and very technical in nature, and measures as well as expertise can be expensive.[74] Simply copying other capacity building measures will not be enough. Second, experts in the field agree that metrics to monitor and evaluate projects not only do not yet sufficiently exist, which not only makes it hard to establish a mutual understanding of what really works (not), but also to show the return on investments to donors and recipients alike. Third, there is often not valid information on the situation on the ground, and because of the security context, some partner countries might not be willing to share relevant information.[75] Country assessments can help define a baseline, but do not yet include follow-up assessments after the implementation of CCB measures. In sum, thorough evaluations, and therefore continued learning, are scarce.

Recommendations

Improve measurement capacities and establish evaluations: Develop transparent, measurable assessment frameworks and metrics to measure progress and assess

72 Muller, *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*. 13.

73 As one of the few donor guidances, UK Cyber Security Capacity Building Programme writes that CCB projects work in their experience best when they "are tied to the HMG [Her Majesty's Government] country strategies; have strong host-government support; take a holistic approach that considers host government digital and cyberpolicies, national strategies, regulation, private sector interests, civil society, technical capability, development context and human rights; take account of what other donors are doing or planning; have co-funding from another country or organisation; and build on previous capacity building projects or partnerships." Government of the United Kingdom, "FCO Cyber Security Capacity Building Programme 2017 to 2018."

74 Interview conducted on Ocober 11, 2016

75 Muller, *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*. 14.

results. These could be based, for example, on the existing maturity indices. On the basis of such metrics, evaluation mechanisms should be integrated into CCB projects. Using the maturity indices, countries could also set up follow-up mechanisms to analyze their progress.

Make the outcome transparent. A learning process needs to take place on the national and international level in order to continually improve CCB outcomes and build on lessons learned. The outcome of individual projects should therefore be communicated in a transparent manner, e.g., though platforms such as the Cybersecurity Capacity Portal or an (expanded) GFCE.

Keep learning while doing. The absence of metrics should not deter actors from taking first steps. While lessons learned from other fields should be taken into account, there is a need for initial projects that aim to build capacity and experience. As one expert put it, "[we should be] building our plane while we are flying it."[76]

Create an annual assessment of the state of CCB. This could be a publication analogous to the "Annual Review of Peace Operations" that reviews key emerging trends, presents lessons learned, and analyzes emerging trends in greater depth.

76 Interview conducted on September 28, 2016

Muddling Through or Keeping Pace?

Over 10 years ago, the signatories of the World Summit on the Information Society (WSIS) outcome documents agreed that "a global culture of cybersecurity need[ed] to be promoted, developed and implemented."[77] Yet in the intervening time we have only seen very gradual progress in the creation of a truly global cybersecurity culture through the joint efforts of governments, companies, academics, and non-profits. Translating this culture into concrete cybersecurity capacity building efforts has occurred at an even slower pace, with the increase in both awareness and CCB failing to keep up with the growth in connectivity. Consequently, global risks have increased while the potential economic and social "digital dividends" have not been fully realized. To change that, we outline specific recommendations above. At this point, it is worth thinking about what is required to take those forward.

Looking Ahead

What will cybersecurity capacity building, at the intersection of development, cybersecurity and diplomacy, look like in the next decade? Continued, exponential growth in connectivity in terms of both users and devices (with the Internet of Things) appears to be a given. Less certain is how cybersecurity and CCB will evolve. To think about different futures and the implications of (not) investing in CCB, we developed two distinct and plausible scenarios:"muddling through" and "keeping pace."

In the "muddling through" scenario, CCB continues to evolve slowly. When increasing connectivity, governments treat security as an afterthought – bypassing costs in the short-term but increasing risks and costs further down the road. A dedicated CCB community pushes ahead, yet without sufficient top-level political attention in Western countries and the necessary growth in resources. At the national and international levels, cultural gaps and turf battles between security, diplomatic, and development actors remain obstacles to effective coordination and cooperation. Without a systematic evaluation capacity, the actors learn slowly – if at all – from failed (and occasionally successful) efforts. Companies continue to have little involvement in CCB, exacerbating the shortage of talent and human capital in the field. Authoritarian digital players such as China will aggressively promote their cybersecurity packages to countries in the Global South, promising tools for cybersecurity and political control

77 *Outcome Documents*. World Summit on the Information Society, 2015. Last accessed on December 21, 2016. http://www.itu.int/net/wsis/outcome/booklet.pdf.

all in one package without any questions asked about dual use – and many governments all too happily taking up the offer.

The "keeping pace" scenario paints a more optimistic future. In this outcome, CCB grows in tandem with connectivity: the next ten years lay the foundations for a true "culture of cybersecurity" to emerge as Western countries invest significantly in cybersecurity, leading by example with reinvigorated cybersecurity progress at home and doubling down on CCB efforts. To this end, they ensure that CCB activities make the best possible use of private sector and non-profit capacities. Western countries all devise clear strategies that security, diplomacy, and development actors work hand in hand to implement. In Europe, national strategies align with concerted CCB efforts at the EU level, and major global development players such as the World Bank dedicate the necessary resources. Projects manage to avoid the pitfalls that have plagued capacity-building efforts in other issue areas. The Global Forum on Cyber Expertise (GFCE) evolves into a true hub for CCB – both empowered to serve as a repository of activities and best practices, and as a means to aid cooperation and coordination between stakeholders. With additional support, the Cybersecurity Capacity Portal is extended to a platform of sharing best practices, which actors regularly turn to provide and receive information on ongoing projects. In this context, existing maturity models are expanded not only to help contextualize different CCB measures, but also to provide a tool for monitoring and evaluating ongoing and past projects. The GFCE or G20 facilitates a stronger role for Global South powerhouses such as India and Brazil to become engaged in CCB. This fosters South-South cooperation as well as trilateral CCB partnerships between Western donors, Southern players such as India, and Global South recipient countries. While not losing sight of privacy and rights concerns, Western countries offer players in the Global South CCB packages that are also attractive to governments who do not want to make privacy and rights protections the number one priority of their digital agenda.

How Germany Can Shape the Next Decade of Cybersecurity Capacity Building

We outline specific recommendations on how to advance CCB above. Yet the deciding factor between these two scenarios is political leadership in terms of (not) pushing for the implementation of a principle-based approach to CCB. There is an opportunity to make use of cybersecurity expertise (which has greatly improved over the last decade) in combination with the knowledge and experience that is available on how (not) to build capacity abroad, especially in the development community. However, without top-level political attention from key countries, the resources necessary for scaling up CCB to keep pace with the anticipated growth in connectivity will not be forthcoming. As the private sector, civil society, and academia continue to contribute to the area, political leaders must support their efforts.

We need robust, sustained engagement from countries such as the Netherlands, the UK, and the US, which have been active in the CCB field already. But we also need new, capable countries to come on board as leaders in the field. There are several factors which indicate that Germany is well placed to take on a key role in the field, even as its CCB efforts are currently still at a nascent stage. The coordination of projects

in Germany has not proven easy, since both the Federal Ministry for Economic Cooperation and the Federal Foreign Office share partially overlapping mandates. At the same time, Germany has one of the world's most advanced ICT systems at a high maturity level,[78] boasts a strong international network, and can build on capacity building efforts in other areas.

Domestic Coordination

To take on a key role, Germany should first lead by example through its domestic setup. In its 2016 cybersecurity stratety, the government already stresses that Germany will support selected partner countries and regions in building preventive and reactive cybersecurity capacities. The strategy recognizes that especially in places where people gain first access to the internet through development activities, "frameworks and knowledge for its secure and reliable use" must be supported.[79] Next, leading by example means devising a clear strategy that cuts across the turf concerns of different ministries and agencies and involves private sector and non-profit players alike. Clear mandates and a compelling strategy need to go hand in hand with a discussion on how to mobilize sufficient funding. The committee for econonomic cooperation and development and the budget committee in the German Bundestag need to consider the issue. The German development bank KfW could also look into funding lines to provide credit for CCB efforts, for example to encourage companies in recipient countries to provide cybersecurity services.

An important question to ask is: who can provide the services that are required? Within the government, there already exists a general need for more IT experts, and it remains to be seen whether relevant ministries and agencies such as the Federal Ministry of the Interior and the Federal Office for Information Security will be able to provide resources for external efforts. Therefore, a real discussion needs to be had on involving experts from the private and non-profit sectors. German technology companies could provide expertise – either as contracting partners or as part of their corporate social responsibilities or research activities. Similar to how the UK government is partnering with – and financially supporting – the Global Cyber Security Capacity Centre (GCSCC) at Oxford University, Germany could partner with domestic universities in specific programs. Building on work done by the Center for International Peace Operations (ZIF), which has tremendous amounts of experience in training and recruiting civilian experts for peace operations, the Geman goverment could develop a similar pool for IT experts. In the broad network of German foundations, there might also be an interest in becoming engaged in specific projects. Independent of who will carry out programs, efforts should be evaluated, and lessons learned should be shared with other stakeholders to help develop best practices going forward.

78 Hathaway et al., *Cyber Readiness Index 2.0*, 2.

79 *Cyber-Sicherheitsstrategie für Deutschland*. Bundesministerium des Inneren, 2016: 42. Last accessed on January 5, 2017. https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile.

International Engagement

Backed by a strong domestic track record, Germany could also become a catalyst for global action. In its relationships with countries in the Global South, Germany would consistently advocate for investing in cybersecurity, thereby helping to address the awareness deficit that still exists among some key players. At the same time, it would help to provide the necessary CCB efforts in countries that have already realized the need to invest in better cybersecurity in order to reap the full benefits of the digital revolution. Additionally, Germany could support the strengthening of multilateral efforts. The European Union is planning to devise a more coherent approach to CCB and is a natural starting point for further discussions.[80] In addition, as the GFCE has posititioned itself as a main international forum for exchange on CCB efforts, Germany could make use of its membership to help the forum become more action-oriened. Either working with the GFCE or through other conferences, the German government could facilitate the exchange between development, cybersecurity, and diplomatic actors to exchange expertise among the different communities. To raise the issue internationally, and to foster South-to-South cooperation, Germany can also use its 2017 G20 presidency to advance the topic at the international level. Since the World Bank is increasing its efforts, there could also be a discussion with other donor countries to provide funding there. Germany could also fund an annual assessment of the state of CCB, similar to the "Annual Review of Peace Operations," that reviews key emerging trends, presents main lessons learned and analyzes emerging trends and themes.

There is a strong case for increasing cooperation and coordination among like-minded nations first. It is in Germany's interest to keep the internet open and free, as well as secure. These values are shared among most Western nations, and will determine the nature of CCB programs. Since trust is an important enabler for cybersecurity cooperation, successful programs are likely going to take place among nations that share similar values. Second, the bar to become a leader in the CCB field is comparatively low. As this study demonstrates, the amount of activities that are currently taking place is low, with extremely limited funding. This makes cybersecurity capacity building not only a field where efforts are vital, but one where Germany could easily have a concrete impact – provided the necessary leadership to pursue a principle-based approach is forthcoming.

80 *Cyber capacity building: towards a strategic European approach, Reference 8732/1/16* Council of the European Union, 2016. Last accessed on January 5, 2017. http://statewatch.org/news/2016/jul/eu-council-cyber-capacity-building-8732-1-16.pdf.

Appendix

Selected Projects[81]

ENCYSEC (Enhancing Cybersecurity: Protecting ICT Networks)[82]

Synopsis: ENCYSEC is a pilot project to increase the security and resilience of ICT networks in the recipient countries by building CSIRTs, developing cybersecurity strategies, and enhancing cooperation
Project consortium: Expertise France (international technical assistance agency and operator for French ministries) and Civipol Conseil (in-house consulting and service company of the French Minister of Interior)
Recipient countries: Macedonia, Moldova and Kosovo
Budget: €1,485 million
Funded by: EU's Instrument contributing to Stability and Peace (IcSP), managed by the Directorate General for International Cooperation and Development (DG DEVCO) of the European Commission.
Duration: January 2014-January 2016 (24 months)
Components:

- CSIRT capacity building;
- Support on establishment or strengthening of operational CSIRT units;
- Facilitation of joint cyber security exercises;
- Advice on development of curriculum for CSIRT officers;
- Cybersecurity strategies and awareness raising;
- Advice on creation and adoption of national cyber security strategies;
- Advice on raising awareness on cyber security, including workshops and conferences for decision makers;
- Enhancing Cooperation: Public-Private Partnerships and International Cooperation;
- Enhance cooperation between government, private sector, and international bodies;
- Advice on updating academic curricula, including computer science and science, technology, engineering, and mathematics;
- Facilitation of CERTS officers in international events.

81 These selected projects aim to provide an idea of how some of the projects have been carried out in the past. They are not representative of the full spectrum of activities.

82 The compilation below is based on nterviews conducted on September 28 and October 5, 2016 as well as information found at: Global Cyber Security Capacity Centre, "Besnik Limaj, Founder and CEO of Logic PLUS and Team Leader of the EU Funded Transregional Project "Enhancing Cyber Security", (March 23, 2015), https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/besnik-limaj-founder-and-ceo-logic-plus-and-team-leader-eu-funded-transregional-project, last accessed on January 5, 2017.; Enhancing Cyber Security, "About ENCYSEC," http://www.encysec.eu/web/, last accessed on January 5, 2017.

GLACY (Global Action on Cybercrime)[83]

Synopsis: GLACY is a joint project of the European Union and the Council of Europe aimed at supporting criminal justice authorities worldwide in partnering to combat cybercrime on the basis of the Budapest Convention on Cybercrime.
Project leaders: Directorate General for International Cooperation and Development (DG DEVCO) of the European Commission and Cybercrime Programme Office of the Council of Europe (C-PROC)
Priority recipient countries: Mauritius, Senegal, Tonga, Morocco, South Africa, Philippines, Sri Lanka
Budget: € 3.35 million
Funding: EU's Instrument contributing to Stability and Peace (IcSP)
Duration: November 1, 2013–October 31, 2016
Components:

- Strategies and engagement of decision-makers;
- Harmonization of legislation;
- Judicial training;
- Law enforcement capacities;
- International cooperation;
- Information sharing;
- Assessment of progress.

Criteria for selecting partner countries:

- Membership of the Budapest Convention (Parties, Signatories, or Invitees);
- Demonstrated political commitment in cybercrime, exemplified by the legislation on cyber issues, potential future capacity, and strategic role in the region.

Example activities:

- Mauritius: International workshop on adaptation of the electronic evidence;
- Senegal: Advisory mission on cybercrime reporting systems;
- Sri Lanka: Instruction for trainers or introductory course on cybercrime and electronic evidence for the judiciary.

Next steps:
GLACY was extended to GLACY+, which runs from March 2016 to February 2020 with the budget of €10 million. On top of the previous recipient countries, GLACY+ also includes Dominican Republic and Ghana as partner countries.

83 The compilation below is based on information found at: Council of Europe, "Global Action on Cybercrime."; Global Forum on Cyber Expertise, "Presentation Annual Meeting 2016 - Global Action on Cybercrime (GLACY)," https://www.thegfce.com/documents/speeches/annual-meeting-2016/06/13/presentation4, last accessed on January 5, 2017.; *Summary of Project Proposal*. Global Action on Cybercrime (GLACY), 2013. Last accessed on January 5, 2017. https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/GLACY/2688_GLACY_summary_v4.pdf.

Internet Infrastructure Initiative[84]

Synopsis: The initiative seeks to broaden the know-how in the area of internet infrastructure and to provide a platform for the sharing of technological solutions, best practices and expertise.

Partner organizations:

- Governments of the Netherlands and Poland;
- Public/Private Platform Internet Standards, The Netherlands
- Kosciuszko Institute, Poland;
- The Netherlands Institute of International Relations 'Clingendael'.

Budget: not available

Duration: 2016 (2–3 years of implementation/ ongoing)

Components:

- Internet standards test tool available in different language versions, building on the website www.internet.nl;
- Capacity building program targeting at implementing the latest versions of internet standards, supported by tutorials, webinars, workshops, tailor-made documentation and knowledge modules.

Organization of American States (OAS) Cybersecurity Program[85]

Synopsis: As one of the overall OAS programs in cybersecurity capacity building, OAS supports its members in establishing national CSIRTs, along with trainings and equipment.

Project leader: Cyber Security Program of the Inter-American Committee against Terrorism (CICTE) of the OAS

Recipient country: All interested OAS members

Budget: not available

Funding: Among others from United Kingdom, Canada and the United States

Duration: 2004–ongoing

Components:

- Development of national cybersecurity strategies;
- Technical training, workshops and country-specific technical missions.
- Cybersecurity exercises;
- Development of national CSIRTs and a regional CSIRT hemispheric network;
- Awareness aising, research and expertise.

---

84 The compilation below is based on information found at: Global Forum on Cyber Expertise, "Internet Infrastructure Initiative," https://www.thegfce.com/initiatives/i/internet-infrastructure-initiative, last accessed on January 5, 2017.; *Internet Infrastructure Initiative*. Global Forum on Cyber Expertise, 2016. Last accessed on January 5, 2017. https://www.thegfce.com/binaries/gfce/documents/speeches/annual-meeting-2016/06/13/presentation7/14.00-14.30-internet-infrastructure-initiative.pdf.

85 The compilation below is based on information found at: *Internet Infrastructure Initiative*. Global Forum on Cyber Expertise. Organization of American States, "Cyber Security."; *OAS Cyber Security Initiative*. Global Forum on Cyber Expertise, 2016. Last accessed on January 5, 2017. https://www.sites.oas.org/cyber/Documents/2015%20OAS%20Cybersecurity%20Initiative.PDF.

Approaches to Assess Cybersecurity Capacity

Several cybersecurity maturity models aim to provide theoretical and practical support in understanding cybersecurity needs, capacities and possibilities for action for individual countries. This recognizes that "the measurement of security postures and progress over time are important elements to strengthening policies, evaluating risks and anticipating future scenarios."[86] Therefore, these models enable the identification of and comparison among national cybersecurity maturity levels. Ideally, they can offer insights into a country's current cybersecurity level and thus enable donor communities to plan and execute CCB measures in a coherent, sustainable way. To gain a better understanding of the existing indexes themselves, we will look at the two of them below – the Potomac Institute's Cyber Readiness Index and Oxford University's Cybersecurity Capacity Maturity Model. Whereas a wider range of indexes exists, due to lack of space we will only take a closer look at two of them. These models stand out because they do not attempt to rank countries, but to truly assess their capacities and provide explicit recommendations on how to improve cybersecurity capacity. An overview and comparison of existing indexes is available at the Cybersecurity Index of Indices.[87]

The Cyber Readiness Index 2.0

Developed by researchers at the Potomac Institute, the Cyber Readiness Index (CRI) aims to evaluate the cybersecurity capabilities of 125 countries that have "embraced [...] ICT and the internet."[88] So far, country reports for the US, France, Japan, Germany, the UK and Italy have been made public.[89] The CRI has two distinct objectives. First, in order enable national leaders and policymakers to make informed assessments on their country's cyber readiness, the index evaluates a country's maturity and dedication to cyber security and resilience. In a second step, the index provides a generally applicable definition of cyber readiness as well as an overview of central features of cyber readiness to provide an "actionable blueprint" for countries to be guided by in their path towards greater levels of readiness.[90] This two-tiered structure aims to inform policy and strategy processes and assess a country's needs in terms of resources, investment, regulatory frameworks or legislative reform.[91]

The index evaluates cyber readiness by analyzing more than 70 indicators along seven categories. Per category, at least 10 indicators are used to assess a country's maturity. The categories are as follows:[92]

---

86 *Cybersecurity Index of Indices*. International Telecommunication Union, 2015. Last accessed on January 5, 2017. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Index_of_Indices_GCI.pdf.

87 Ibid.

88 Hathaway et al., *Cyber Readiness Index 2.0*, 2.

89 Potomac Institute for Policy Studies, "Cyber Readiness Index," http://www.potomacinstitute.org/academic-centers/cyber-readiness-index, last accessed on January 5, 2017.

90 Hathaway et al., *Cyber Readiness Index 2.0.* , 3.

91 Ibid., 3-4.

92 Ibid., 6.

1. **National strategy:** The first and most important element of the CRI's assessment of a country's cyber preparedness focuses on the articulation of that country's cyber strategy (or lack thereof). The index identifies several characteristics of sound national cyber strategies that include but are not limited to:
- The publication of a national cyber security strategy that is inclusive of economic opportunities and risks associated with ICT uptake;
- The designation of a competent authority and the clear delineation of its positional authority;
- The identification of the financial and human resources requested and allocated for the implementation of the strategy;
- The identification of the mechanisms required to secure critical cyber infrastructure and ICT uptake;

2. **Incident response:** A second element indicating a country's preparedness is, according to the CRI, its response to cyber incidents. Organized incident response often takes the form of CSIRTs, which may be but are not always governmentally organized. Factors to gauge a country's readiness regarding cyber incidents include:
- The publication of an incident response plan for emergencies and crises;
- The establishment of a national CSIRT to manage incident response and serve a broad national constituency (beyond government and critical infrastructure providers);
- The identification of the financial and human resources requested and allocated for the National CSIRT to carry out its mandate;
- A demonstrated capability in the incident containment, management, resilience, and recovery processes for critical services and infrastructures.

3. **E-crime and law enforcement:** The third category featured in the CRI pertains to a country's organization of defense against cyber crime and fraud and corresponding law enforcement activities. As cybercrime transcends national borders, the index attributes special importance to this element. Important characteristics of a sound national response strategy in line with international commitments to cyber crime include:
- A demonstrated commitment to establish national legal and policy mechanisms to specifically reduce the criminal activity emanating from the country and promote coordination mechanisms to address international and national cyber crime;
- The establishment of a mature institutional ability to fight cybercrime, including training for court judges, prosecutors,lawyers, law enforcement officials, forensic specialists, and other investigators;
- The identification of financial and human resources requested and allocated for fighting cybercrime;
- Demonstrable evidence of a country's commitment to review and update existing laws and regulatory governance mechanisms, identify where gaps and overlapping authorities may reside, and clarify and prioritize areas that require modernization (e.g., existing laws, such as old telecommunications law).

4. **Information sharing:** Information sharing relates to the ability of a country to establish and maintain well-functioning mechanisms for intelligence sharing among relevant government agencies and industry stakeholders. Factors by which to measure this include:

- The articulation and dissemination of a policy on information sharing across sectors that enables the exchange of actionable intelligence/information between governments and industry sectors;
- The identification of an institutional structure that transmits authoritative information from government sources to government agencies and critical industries;
- The identification of the financial and human resources requested and allocated for government-driven authoritative information exchange or other institutional structure(s) dedicated to the information sharing mechanisms;
- Demonstrable evidence that cross-sector and cross-stakeholder coordination mechanisms meant to address critical interdependencies – including incident situational awareness and cross-sector and cross-stakeholder incident management – are adequately maintained and tested for effective performance.

5. **Investment in research and development (R&D):** The fifth category employed by the CRI related to a country's preparedness to establish research and development facilities regarding ICTs more broadly. This is assessed with regard to:

- A publicly announced commitment by the government to invest nationally in basic and applied cyber security research;
- The identification of at least one entity with the responsibility to oversee national cyber security R&D initiatives and serve as a national and international point-of-contact for collaboration;
- The identification of financial and human resources requested and allocated for cyber security basic and applied research and initiatives;
- The implementation of programs dedicated to the development, dissemination, and routinization of interoperable and secure technical standards, acceptable to and reinforced by internationally recognized standards bodies.

6. **Diplomacy and trade:** The sixth criterion relates to the incooperation of cyber issues in a country's trade and foreign policies. This is assessed with regard to the following elements:

- The announced identification of cyber security as an essential element of foreign policy and national security (e.g. Official discussions typically involving high-level political and military leaders in bilateral and multilateral discussions);
- The establishment of dedicated and trained personnel in the country's foreign office or equivalent organization whose primary mission includes active engagement internationally in cyber security diplomacy;
- The identification of the financial and human resources requested and allocated for cyber diplomatic engagement;
- Demonstrated participation in defining, signing, and enforcing international, multi-national, regional and/or bilateral agreements pursuing mutually acceptable solutions to common challenges.

7. **Defense and crisis response:** The final element used by the CRI relates to a country's cyber defense and response to cyber-associated crises. Features used to assess such capacities are:

- The publication of national statements that assign an organization the national cyber defense mission as a top tier mission;
- The establishment of a national-level organization, within the military, whose primary mission is the cyber defense of the nation;
- The identification of financial and human resources requested and allocated for the organization, within the military, whose mission explicitly includes the cyber defense of the nation;
- Evidence of conducted government-level exercises that demonstrate national cyber defense readiness.

The index's assessment of a country's cyber readiness, relies on various inputs such as interviews and an analysis of national strategic documents. Assessments are categorized into three levels of cyber preparedness: insufficient evidence, partially operational and fully operational. With regard to the sample consisting of 125 countries, the index aims at reflecting a diverse and representative sample, featuring countries of diverse economic development level, regional origin and trade affiliations.

The Cyber Readiness Index stands out through its broad geographic range, even though most of the country assessments still need to be published. While extensive in the range of countries covered, it is limited in so far as the CRI's methodology is only applicable to the cyber readiness of countries rather than organizations, government institutions or regions. The CRI does not only assess the technical maturity of a country's cyber capacities but also attempts to evaluate a country's overall commitment to cyber issues – an important albeit much harder to quantify aspect of cyber maturity.

The Cybersecurity Capability Maturity Model

Compiled by researchers at the Global Cyber Security Capacity Center at the Oxford Martin School, the Cyber Security Capability Maturity Model (CMM) is one of the most comprehensive efforts to assess a country's national cybersecurity capabilities. Similar to the CRI and other indices, the CMM aims at providing a better understanding of cybersecurity capacities in order to support policymakers by underpinning their cybersecurity strategies with empirical assessments of a country's or organization's cybersecurity needs.[93]

The CMM understands cybersecurity capacities to comprise five dimensions, depicted in graph 1 above.[94] Because these dimensions are rather wide, each dimension is made up of several factors that together make up one dimension.[95]

---

93 *Cyber Security Capability Maturity Model (CMM) – V1.2*. Global Cyber Security Capacity Centre, 2014: 3. Last accessed on December 9, 2016. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf.

94 Ibid., 3.

95 Global Cyber Security Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition" (February 9, 2017), https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf, last accessed on February 25, 2017.

1. Devising Cybersecurity Policy and Strategy
- D1-1: National Cybersecurity Strategy;
- D1-2 Incident Response;
- D1-3: Critical National Infrastructure (CNI) Protection;
- D1-4: Crisis Management;
- D1-5 Cyber Defence;
- D1-6 Communications Redundancy.

2. Cyber Culture and Society
- D2-1: Cybersecurity Mind-set;
- D2-2: Trust and Confidence on the Internet;
- D2-3: User Understanding of Personal Information Protection Online;
- D2-4: Reporting Mechanisms;
- D2-5: Media and Social Media.

3. Cyber Security Education, Training, and Skills
- D3-1: Awareness Raising;
- D3-2: Framework for Education;
- D3-3: Framework for Professional Training.

4. Legal and Regulatory Frameworks
- D4-1: Legal Frameworks;
- D4-2: Criminal Justice System;
- D4-3: Formal and Informal Cooperation Frameworks to Combat Cybercrime.

5. Standards, Organiations, and Technologies
- D5-1: Adherence to Standards;
- D5-2: Internet Infrastructure Resilience;
- D5-3: Software Quality;
- D5-4: Technical Security Controls;
- D5-5: Cryptographic Controls;
- D5-6: Cybersecurity Marketplace;
- D5-7: Responsible Disclosure.

Naturally, maturity levels may vary greatly across different factors and dimensions. Maturity is categorized in five levels:[96]

- "Start-up: At this level either nothing exists, or it is very embryonic in nature. It could also include initial discussions about cyber capacity building, but no concrete actions have been taken. It also includes a lack of observed evidence in this particular indicator.

96 Cyber Security Capability Maturity Model (CMM) – V1.2. Global Cyber Security Capacity Centre, 2014: 3-4. Last accessed on December 9, 2016. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf

- Formative: Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined - or simply "new." However, evidence of this activity can be clearly evidenced.

- Established: The elements of the sub-factor are in place, and working. There is not, however, well-thought out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the *relative* investment in the various elements of the sub-factor. But the indicators is functional and defined.

- Strategic: Choices have been made about which parts of the indicator are important, and which are less important for the particular organization/nation. Of course, we would all like everything to be as important as everything else, but with finite resources, choices must be made. The strategic level reflects the fact that these choices have been made. They should have been made contingent on the nation/organization's particular circumstances.

- Dynamic: At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances: for example, the technology of the threat environment, global conflict, a significant change in one area of concern (e.g. Cybercrime or privacy). Dynamic organizations have developed methods for changing strategies in stride,in a "sense-and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this level."

By categorizing cybersecurity maturity in five specific and detailed dimensions, the CMM offers decision makers a way to assess the cybersecurity maturity of their country while offering a good blueprint of what it takes to achieve the respective next higher level of maturity. The factors comprising different levels of cybersecurity maturity do not act as isolated criteria within their dimension but rather interact across levels and thus make for a dynamic model.

Beyond serving as an important resource, the model has other functions too: the team at the GCSCC has also been carrying out various country assessments, such as Kosovo,[97] Bhutan,[98] the UK[99] and Senegal.[100,101] The reports are made public if the

97 Maria Bada, *Cybersecurity Capacity Assessment of the Republic of Kosovo*. Global Cyber Security Capacity Centre, 2015. Last accessed on January 5, 2017. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Kosovo_June_2015.pdf.

98 Taylor Roberts, *Building Cyber-security Capacity in the Kingdom of Bhutan*. Global Cyber Security Capacity Centre, 2015. Last accessed on January 5, 2017. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Bhutan_September_2015.pdf.

99 Maria Bada, *Cybersecurity Capacity Review of the United Kingdom*.

100 Taylor Roberts and Eva Ignatuschtschenko, *Cybersecurity Capacity Review of the Republic of Senegal*. Global Cyber Security Capacity Centre, 2016. Last accessed on January 5, 2017. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Senegal-Report-v4%20.pdf.

101 The CMM was also applied in the OAS member states in 2015 and a joint report published with the Inter-American Development Bank in 2016 entitled ' 'Cybersecurtiy: Are we ready in Latin America and the Caribbean'. An interactive version is accessible at www.cybersecurityobservatory.com, last accessed January 18, 2017.

country agrees. It is important to stress that these assessments not only provide a basis for the country itself to prioritize next steps, and for donor countries to tailor CCB measures. The assessment process also brings together a variety of national stakeholders to provide input, often is an important (first) step in moving forward national cybersecurity capacity.

References

Bada, Maria, *Cybersecurity Capacity Assessment of the Republic of Kosovo*. Global Cyber Security Capacity Centre, 2015. Accessed January 5, 2017. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Kosovo_June_2015.pdf.

Bada, Maria, *Cybersecurity Capacity Review of the United Kingdom*. Global Cyber Security Capacity

Centre, 2016. Accessed January 5, 2017. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf.

Bauer, Johannes M., and William H. Dutton, *The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet*. World Bank, 2015. Accessed December 12, 2016. https://openknowledge.worldbank.org/bitstream/handle/10986/23641/WDR16-BP-The-New-Cybersecurity-Agenda-Bauer-Dutton.pdf;sequence=1.

Bolger, Joe, *Capacity Development: Why, What and How*. Canadian International Development Agency,

2000. Accessed December 9, 2016. http://www.hiproweb.org/fileadmin/cdroms/Biblio_Renforcement/documents/Chapter-1/Chap1Doc1.pdf.

Bundesministerium des Inneren, *Cyber-Sicherheitsstrategie für Deutschland* [Cyber-security Strategy for Germany]. 2016. Accessed January 5, 2017. https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile.

Burt, David, Paul Nicholas, Travis Scoles, and Kevin Sullivan, *The Cybersecurity Risk Paradox: Measuring the Impact of Social, Economic, and Technological Factors on Rates of Malware*. Microsoft Security Intelligence Report, 2014. Accessed January 2, 2017. https://blogs.microsoft.com/microsoftsecure/2014/01/16/the-cybersecurity-risk-paradox-measuring-the-impact-of-social-economic-and-technological-factors-on-cybersecurity/.

Buss, Ilka N., *Best Practices in Capacity Building Approaches*. Deutsche Gesellschaft für Technische Zusammenarbeit, 2010. Accessed December 21, 2016. http://ledsgp.org/wp-content/uploads/2015/07/Best-Practices-in-Capacity-Building-Approaches.pdf.

Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Report Summary*. 2014. Accessed January 2, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf.

Council of Europe. "Global Action on Cybercrime." ALccessed on January 2, 2017. http://www.coe.int/en/web/cybercrime/glacy.,

Council of Europe, *Summary of Project Proposal*. Global Action on Cybercrime (GLACY), 2013. LastA accessed on January 5, 2017. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/GLACY/2688_GLACY_summary_v4.pdf.https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/GLACY/2688_GLACY_summary_v4.pdf.

Council of the European Union, *Cyber capacity building: towards a strategic European approach, Reference 8732/1/16*. 2016. Accessed January 5, 2017. http://statewatch.org/news/2016/jul/eu-council-cyber-capacity-building-8732-1-16.pdf.

Department of Homeland Security. "What Is Security and Resilience?" 2016. ALccessed January 2, 2017. https://www.dhs.gov/what-security-and-resilience.

Enhancing Cyber Security. "About ENCYSEC." ALccessed January 5, 2017. http://www.encysec.eu/web/.

European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 2013. ALast accessed on January 5, 2016. http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

Global Cyber Security Capacity Centre. "Besnik Limaj, Founder and CEO of Logic PLUS and Team Leader of the EU Funded Transregional Project "Enhancing Cyber Security"." 2015. ALccessed January 5, 2017. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/besnik-limaj-founder-and-ceo-logic-plus-and-team-leader-eu-funded-transregional-project.

Global Cyber Security Capacity Centre, *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition*. February 9, 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20

edition_09022017_1.pdf.*Cyber Security Capability Maturity Model (CMM) – V1.2*. 2014. Last accessed on December 9, 2016. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf

Global Cyber Security Capacity Centre. "Cybersecurity Capacity of the UK," 2016. ALast accessed on January 6, 2016. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-uk.

Global Cyber Security Capacity Centre. "A Global Resource for Cybersecurity Capacity Building." ALast accessed on January 3, 2017.https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front.

Global Forum on Cyber Expertise. "Coordinated Vulnerability Disclosure." ALast accessed on January 2, 2017.

https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking.

Global Forum on Cyber Expertise. "CSIRT Maturity Initiative." ALast accessed on January 2, 2017. https://www.thegfce.com/initiatives/c/csirt-maturity-initiative.

Global Forum on Cyber Expertise. "CyberGreen." ALast accessed on January 3, 2017. https://www.thegfce.com/initiatives/c/cybergreen.

Global Forum on Cyber Expertise. "Global Campaign to Raise Cybersecurity Awareness." ALast accessed on January 2, 2017. https://www.thegfce.com/initiatives/g/global-campaign-to-raise-cybersecurity-awareness.

Global Forum on Cyber Expertise *, The Hague Declaration on the GFCE*. 2015. ALast accessed on January 2, 2017. https://www.thegfce.com/about/documents/publications/2015/04/16/the-hague-declaration-on-the-gfce.

Global Forum on Cyber Expertise. "Initiatives." ALast accessed on January 2, 2017.

https://www.thegfce.com/initiatives.

Global Forum on Cyber Expertise*, Internet Infrastructure Initiative*. 2016. ALast accessed on January 5, 2017. https://www.thegfce.com/binaries/gfce/documents/speeches/annual-meeting-2016/06/13/presentation7/14.00-14.30-internet-infrastructure-initiative.pdf.

Global Forum on Cyber Expertise, *Internet Infrastructure Initiative*. ALast accessed on January 5, 2017.

https://www.thegfce.com/initiatives/i/internet-infrastructure-initiative.

Global Forum on Cyber Expertise*, OAS Cyber Security Initiative*. 2016. ALast accessed on January 5, 2017. https://www.sites.oas.org/cyber/Documents/2015%20OAS%20Cybersecurity%20Initiative.PDF.

Global Forum on Cyber Expertise. "Overview Members." Accessed January 2, 2017. https://www.thegfce.com/organization/members/overview-members.

Global Forum on Cyber Expertise. "Presentation Annual Meeting 2016 - Global Action on Cybercrime (GLACY)." ALast accessed on January 5, 2017. https://www.thegfce.com/documents/speeches/annual-meeting-2016/06/13/presentation4.

Global Forum on Cyber Expertise. "Promoting Cybersecurity Due Diligence across Africa." ALast accessed on January 2, 2017. https://www.thegfce.com/initiatives/p/promoting-cybersecurity-due-diligence-across-africa.

Global Forum on Cyber Expertise. "Vision and ambition." Accessed January 2, 2017. https://www.thegfce.com/about/contents/vision.

Government of the United Kingdom. *FCO Cyber Security Capacity Building Programme 2017 to 2018*. ALast accessed on January 3, 2017. https://www.gov.uk/government/publications/fco-cyber-security-capacity-building-programme-2017-to-2018.

Government of the United Kingdom*, National Cyber Security Strategy 2016-2021*. 2016. ALast accessed on January 3, 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Government of the United Kingdom. "Oxford will host Cyber Security Capacity Building Centre," 2013. ALast accessed on January 3, 2017. https://www.gov.uk/government/news/oxford-will-host-cyber-security-capacity-building-centre.

Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri, *Cyber Readiness Index 2.0*. Potomac Institute for Policy Studies, 2015. Accessed December 21, 2016. http://www.potomacinstitute.org/images/CRIndex2.0.pdf.

International Telecommunication Union. "About ITU." ALast accessed on January 2, 2017. http://www.itu.int/en/about/Pages/default.aspx.

International Telecommunication Union*, Cybersecurity Index of Indices*. 2015. A Last accessed on January 5, 2017. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Index_of_Indices_GCI.pdf.

International Telecommunication Union. *ICT Facts and Figures 2016*. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf

International Telecommunication Union. "ICTs for a Sustainable World #ICT4SDG." ALast accessed on January 2, 2017.http://www.itu.int/en/sustainable-world/Pages/default.aspx.

International Telecommunication Union. "ITU-EC-ACP Project." ALast accessed on January 2, 2017. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx.

International Telecommunication Union. *ITU-Impact, Applied Learning for Emergency Response Teams (ALERT)*. 2013. Last aAccessed on January 2, 2017. https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/ITU-IMPACT%20ALERT.pdf.

International Telecommunication Union*, Outcome Documents*. World Summit on the Information Society, 2015. Last aAccessed on December 21, 2016. http://www.itu.int/net/wsis/outcome/booklet.pdf.

Klimburg, Alexander, and Hugo Zylberberg, *Cyber Security Capacity Building: Developing Access*. Norwegian Institute of International Affairs, 2015. Accessed December 21, 2016. https://www.files.ethz.ch/isn/195765/NUPI_Report_6_15.pdf.

Krebs, Brian. "Did the Mirai Botnet Really Take Liberia Offline?" *Krebs On Security*, 2016. https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-really-take-liberia-offline/, Accessed January 2, 2017.

Muller, Lilly Pijnenburg *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*, ed. Norwegian Institute of International Affairs. 2015. Accessed December 9, 2016. https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf.

DF.National Cyber Security Centre. "What is the NCSC?" Last accessed onAccessed January 2, 2017.

https://www.ncsc.nl/english/organisation.

Organization of American States. "Cyber Security." Last accessed onAccessed January 3, 2017 https://www.sites.oas.org/cyber/en/pages/default.aspx.

.Organisation for Economic Co-operation and Development, *The Challenge of Capacity Development: Working Towards Good Practice*. 2006. Last accessed onAccessed December 21, 2016. http://www.fao.org/fileadmin/templates/capacitybuilding/pdf/DAC_paper_final.pdf.

Organisation for Economic Co-operation and Development*, The Paris Declaration on Aid Effectiveness*. 2005. Accessed January 2, 2017. https://www.oecd.org/dac/effectiveness/34428351.pdf.

Organisation for Economic Co-operation and Development*, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*. 2015. Last accessed onAccessed December 12, 2016. http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=328&InstrumentPID=371&Lang=en&Book=False.

Pawlak, Patryk. "Capacity Building in Cyberspace as an Instrument of Foreign Policy." *Global Policy* 7, no. 1 (2016).

Pawlak, Patryk, *Cyber Capacity Building in Ten Points*. European Union Institute for Security Studies, 2014. Accessed December 9, 2016. http://www.iss.europa.eu/uploads/media/EUISS_Conference-Capacity_building_in_ten_points-0414.pdf.

Pawlak, Patryk, *Riding the digital wave: the impact of cyber capacity building on human development*, ed. Patryk Pawlak. European Union Institute for Security Studies, 2014. Accessed December 21, 2016. http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf.

Pernik, Piret, Jesse Wojtkowiak, and Alexander Verschoor-Kirss, *National Cyber Security Organisation: UNITED STATES*. NATO Cooperative Cyber Defence Centre of Excellence, 2016. Accessed January 2, 2017. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf.

Potomac Institute for Policy Studies. "Cyber Readiness Index." Last accessed onAccessed January 5, 2017. http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

Raines, Paul. "Re-thinking development aid in the digital age." *CSO Online*, 2015. Last accessed onAccessed January 2, 2017. http://www.csoonline.com/article/2878566/cyber-attacks-espionage/re-thinking-development-aid-in-the-digital-age.html.

Raines, Paul. "UNDP Cybersecurity Assistance for Developing Nations." *CSO50 Confab*, 2016. Last accessed onAccessed January 2, 2017. http://www.csoconfab.com/wp-content/uploads/2016/03/CSO50_2016_Paul-Raines_Providing-Effective-Cybersecurity.pdf.

Roberts, Taylor, *Building Cyber-security Capacity in the Kingdom of Bhutan*. Global Cyber Security Capacity Centre, 2015. Accessed January 5, 2017. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Bhutan_September_2015.pdf.

Roberts, Taylor, and Eva Ignatuschtschenko, *Cybersecurity Capacity Review of the Republic of Senegal*. Global Cyber Security Capacity Centre, 2016. Accessed January 5, 2017.

https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Senegal-Report-v4%20.pdf.

Schia, Niels Nagelhus, *'Teach a person how to surf': Cyber security as development assistance*. Norwegian Institute of International Affairs, 2016. Accessed January 5, 2017. https://brage.bibsys.no/xmlui/bitstream/id/415569/NUPI_Report_4_16_Nagelhus_Schia.pdf.

Schjølberg, Stein, *Report of the Chairman of HLEG*. ITU Global Cybersecurity Agenda (GCA), 2008. Accessed December 12, 2016. http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf.

U.S. State Department of State. "Office of the Coordinator for Cyber Issues." Last accessed onAccessed January 2, 2017.

https://www.state.gov/s/cyberissues/.

U.S. Department of State*, Department of State International Cyberspace Policy Strategy.* 2016. Last accessed onAccessed January 3, 2017. https://www.state.gov/documents/organization/255732.pdf.

United Nations Development Programme, *Basics of Capacity Development for Disaster Risk Reduction*. 2012. Last accessed onAccessed January 2, 2017. http://www.undp.org/content/undp/en/home/librarypage/crisis-prevention-and-recovery/basics-of-capacity-development-for-disaster-risk-reduction-.html.

United Nations Development Programme. "'Seoul framework' could make cyberspace safer, more accessible." 2013. Last accessed onAccessed January 2, 2017. http://www.undp.org/content/seoul_policy_center/en/home/presscenter/articles/2013/10/18/-seoul-framework-could-make-cyberspace-safer-more-accessible-.html

United Nations General Assembly*, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. 2013. Last accessed onAccessed December 21, 2016. https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf.

United Nations General Assembly*, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. 2015. Last accessed onAccessed December 12, 2016. https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf.

United Nations News Centre. "Internet well on way to 3 billion users, UN telecom agency reports." 2014. Last accessed onAccessed December 12, 2016. http://www.un.org/apps/news/story.asp?NewsID=47729#.WE504iQkyUl.

United Nations Office on Drugs and Crime*, Comprehensive Study on Cybercrime*. 2013. Last accessed onAccessed January 5, 2017. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

United Nations Office on Drugs and Crime*, UNODC Annual Report 2015*. 2015. Accessed January 5, 2017. http://www.unodc.org/documents/AnnualReport2015/Annual_Report_2016_WEB.pdf.

Walters, Hettie, *Capacity Development, Institutional Change and Theory of Change: What do we mean and where are the linkages*. Wageningen International, 2007. Accessed December 12, 2016. http://portals.wi.wur.nl/files/docs/successfailuredevelopment/Walters_CapacityDevelopmentConceptPaperFIN.pdf.

The White House *, International Strategy for Cyberspace*. 2011. Last accessed onAccessed January 6, 2016. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

World Bank. *Digital Development Partnership*. 2016. Last accessed on January 2, 2017. http://cwi.unik.no/images/8/8c/DDP_partnership_brochure_draft22Jun2016.pdf.

World Bank *, Digital Dividends, Flagship Report*. 2016. Last accessed onAccessed December 21, 2016. http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.

World Economic Forum*, Expanding Participation and Boosting Growth: The Infrastructure Needs of the Digital Economy*. 2015. Last accessed onAccessed January 2, 2017. http://www3.weforum.org/docs/WEFUSA_DigitalInfrastructure_Report2015.pdf.

Global Public Policy Institute (GPPi)
Reinhardtstr. 7, 10117 Berlin, Germany
Phone +49 30 275 959 75-0
Fax +49 30 275 959 75-99
gppi@gppi.net

gppi.net