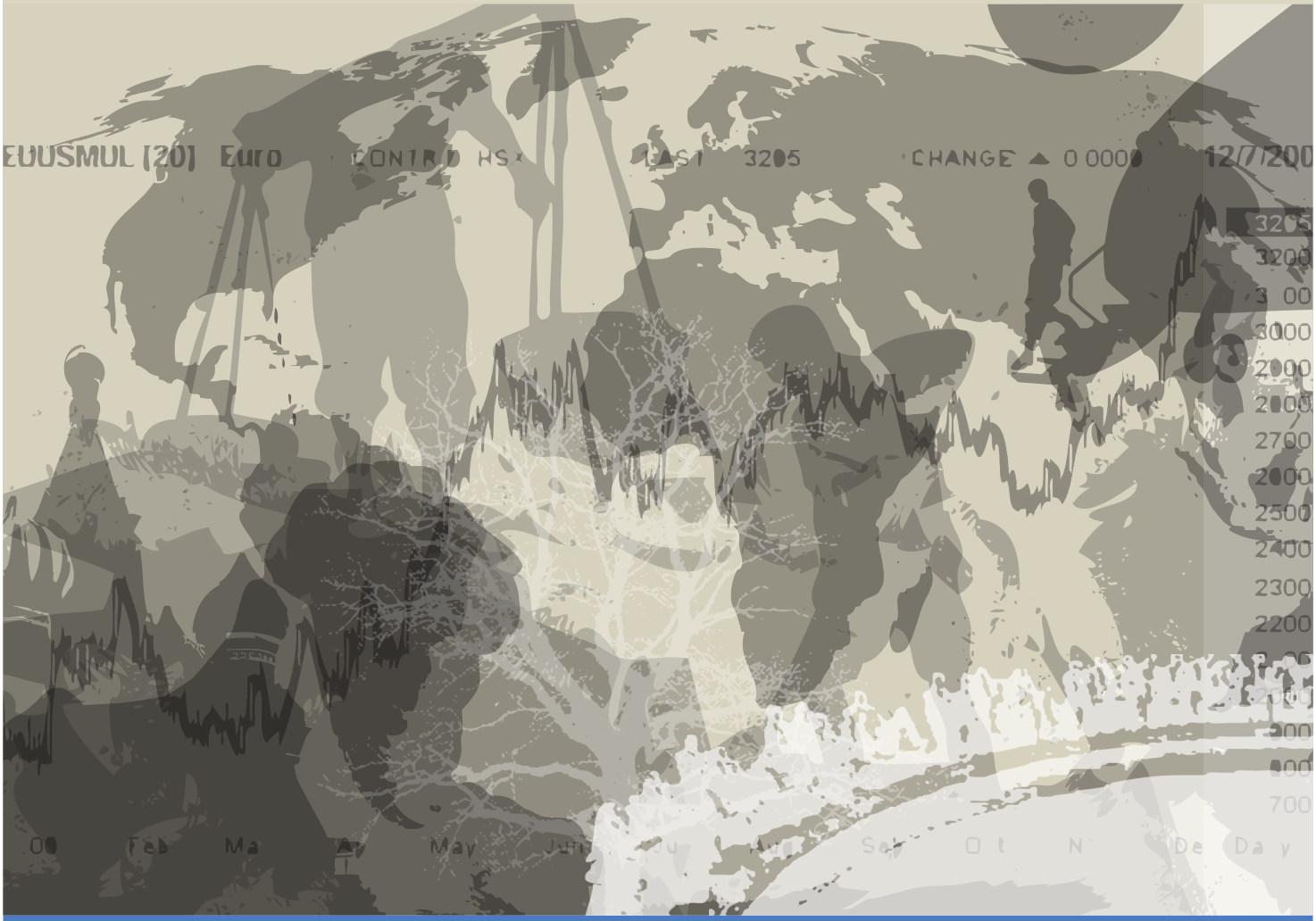
Norwegian Institute of International Affairs

‘Teach a person how to surf’: Cyber security as development assistance

Niels Nagelhus Schia



NUPI Report
[Report no. 4, 2016]

Publisher: Norwegian Institute of International Affairs

ISSN: 1894-650X

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

‘Teach a person how to surf’

Cyber security as development assistance

Niels Nagelhus Schia

Published by Norwegian Institute of International Affairs

Contents

Introduction

Much policy literature on digitalization and development has focused on the importance of connecting developing countries to digital networks, and how such technology can expand access to information for billions of people in developing countries, stimulating economic activity, collaboration and organizations. Good connection to digital networks may have a fundamental impact on societies, changing not only how individuals and businesses navigate, operate and seek opportunities, but also as regards relations between government and the citizenry. Instead of adding to the substantial literature on the potential dividends, this report examines a less-studied issue: the new societal vulnerabilities emerging from digitalization in developing countries. While there is wide agreement about the need to bridge the gap between the connected and the disconnected, the pitfalls are many, especially concerning cyber security[1] – a topic often neglected, also in the recent World Bank report *Digital Dividends* (2016).

The present report is an attempt at redressing this imbalance. Firstly, I contextualize security concerns by briefly describing the historical trajectory of digitalization in developing countries and how it diverges from that of the developed countries. Selected empirical snapshots are presented to describe the current situation in several developing countries. This contextualization exercise provides the backdrop for the second section, which explores how 'technological leapfrogging' in developing countries creates new societal vulnerabilities different from those in the industrialized world, and argues that cyber security needs to become an integral part of development if the UN's Sustainable Development Goals (SDGs) are to be achieved. In the third section I contextualize the 'ownership' debate from the development sector to the cyber field. Measures for building cyber security capacity must exceed prescribed standards, values and subscription numbers, in order to capture the social and economic context in which digitalization occurs. Finally, I turn to how the public–private relationship in the field of digitalization puts 'ownership' in a new light.

---

1 Cyber security is closely interlinked with the security of cyberspace; it is broadly understood and involves a multitude of actors in this text. The link between cyber security and national security is well established and uncontested. Myriam Dunn Cavelty's broad definition is used here: it refers to cyber security in the technical sphere as: '… a multifaceted set of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access, in accordance with the common information security goals: the protection of confidentiality, integrity, and availability of information.' In the national setting it refers to 'the security one enjoys in and from cyberspace' (Cavelty, forthcoming 2016: 2–3)

Rationale

Digital technology underpins most of the social, economic and political development goals of most donor countries and international organizations today. Cyber Security Capacity Building (CCB), an approach aimed at advancing, cultivating and encouraging growth and stability in developing countries through digitalization, seems set to play an increasingly important role in future foreign-policy considerations and government programmes.[2]

In the NUPI project 'Cyber Security Capacity Building' (2015–2016) we have mapped out concrete risks and challenges, produced recommendations for dealing with them and provided suggestions for implementing these tools effectively. (In addition to the present project report, see Klimburg and Zylberberg 2015, Muller 2015, and Langø 2016.) These three reports provide micro-perspectives, through in-depth assessment of various angles of specific issues pertaining to cyber security. The present summarizing report draws on these reports in addition to recent research, offering an up-to-date research assessment of the overall picture: the macro-perspective. Among the questions pursued in the NUPI project were:

- What are the extent and nature of cyber challenges in developing countries?
- How does this affect Western security?
- Do various countries' cyber security models share certain features that can be replicated in developing countries?
- How do the roles and mandates of various government agencies, the private sector and the civil society in industrialized countries *differ*?
- Could there be a conflict between Western and developing countries' security interests in these models?
- What has been done in terms of capacity building? – *a mapping exercise*
- What are the context-dependent technical, political, governmental, societal and economic factors that need to be taken into account?

---

2 CCB was initially more concerned with economic issues, followed by international security agendas and human rights. The development context is the latest addition to this field (see Klimburg and Zylberberg 2015: 5)

This report draws on and further develops the analyses of these questions presented in the other three reports, in order to assess the extent to which CCB in developing countries has merit, and whether effects have been limited to the regional environment or are more global in reach. The first project report 'Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities' (Muller 2015) focuses on challenges to implementation of cyber security, offering an overview and discussion of different approaches to CCB. The second project report, 'Cyber Security Capacity Building: Developing Access' (Klimburg and Zylberberg 2015), provides a rationale and identifies potential dimensions for governmental cyber security capacity building and what tasks they should cover. Frameworks and recommendations for assessing and delivering CCB programmes are outlined. The third project report 'Cyber Security Capacity Building: Security and Freedom' (Langø 2016) is concerned with the intersection of technology and politics in developing countries, and in particular with digitalization in developing countries in transitions towards democracies.

Drawing on the project findings and the three reports, the present report concludes with some overall recommendations for policymakers regarding possible Norwegian involvement in building cyber security capacity in the developing world.

The NUPI project has identified three main reasons why CCB will be increasingly important for the *development–security nexus*: 1) Access to cyberspace is essential to social, economic and political stability, so the importance of, and need for, CCB measures and programmes for regional stability will grow. 2) Developing countries are increasingly becoming host to the infrastructure and actors behind malicious cyber activities. Bridging the digital divide is important also with regard to responding to national security and various types of cyber threats in donor countries. 3) The international debate about governing the Internet is becoming increasingly politicized. Many developing countries hold swing-state positions in this political landscape, and their influence and importance are likely to grow (Klimburg and Zylberberg 2015). Thus, CCB seems set to become an increasingly important arena for international diplomacy. Furthermore, because of the increasing dependence on cyber space in all sectors of society around the world, it is important to have a holistic and comprehensive approach to new questions raised by the digital technological revolution. Norway has the comparative advantage of a long track record within the development industry, but also as regards multilateral diplomatic negotiations. Combining these two dimensions could offer great potentials for strengthening Norwegian long-term interests such as the production of new norms, as well as following up on SDG commitments by contributing to the digital revolution in developing countries.

Background

Information and communication technology (ITC) is nothing new. The first undersea telegraph cable /under the Atlantic Ocean/ was laid in 1858 by the Atlantic Telegraph Company. The International Telecommunication Union (ITU) was founded in 1865, and became a UN agency in 1947. The ARPANET (predecessor to the Internet) was created in 1969; the first email was sent in 1971; the first Internet worm or malware was detected in 1988; and in 1993, the Internet and the World Wide Web were made publicly accessible and free. Although information and communication technology has been around for more than a century, digitalization and cyber space represent a fairly new field in international politics (global economic, security and human rights agendas), even more recent in the field of development politics.

In 1999, the first UN resolution addressing cyber security was adopted, marking the starting point for a multilateral, intergovernmental effort to address cyber security. The first UN resolution pertaining to digitalization and development came in 2001, when the General Assembly decided that a World Summit on the Information Society (WSIS) should be held. The first meeting took place in Geneva in 2003, the second meeting in Tunis in 2005; these were followed up by a WSIS+10 in New York in 2015. Because the goal of the first meeting was to provide the foundations for an information society for all, this meeting had implications for development politics as well.[3] In 2004, the Partnership on Measuring ICT for Development was launched as a multi-stakeholder initiative to improve the situation in developing countries. In Tunis in 2005, the second WSIS meeting emphasized implementation and financing mechanisms, as well as Internet governance. Multiple stakeholders broadly supported the outcome resolution of the Geneva and the Tunis meetings. Since then, and particularly in the last five years, the pace of policymaking has increased rapidly. Highways for policymaking have been produced, especially as regards *cyber security*, *cyber crime* and *Internet governance*. Now the *cyber and development highway* also seems to be gaining momentum. In 2015, the WSIS+10 High-level meetings made recommendations on how to proceed so as to further connect developing countries, and called on all '... governments, the private sector, civil society, international organizations, the technical and academic communities and all other relevant stakeholders to integrate information and communication technologies (ICTs) in their implementation approaches to the SDGs' (WSIS 2015: bullet point 17).

---

3 175 countries were represented, together with international organizations, private sector and civil society at the meeting in Geneva, where they endorsed the Geneva Declaration of Principles and Geneva Plan of Action, adopted 12. December 2003.

The 2030 agenda for sustainable development goals (SDG), adopted by the United Nations on 25 September 2015, was designed to combat poverty, inequality and climate change. These overarching goals, further specified into 17 goals and 169 targets, are by many seen in conjunction with the spread of new technology (see for instance World Bank 2016, Bildt 2015). New ITCs are contributing to growth and development in developing countries through increased productivity, by providing public and private services to people in rural and poor areas and by promoting new economic and social opportunities to people living in developing countries. The connections between technology and growth have also been confirmed through statistics on the use of information technology and the extent to which countries are connected correlates with increases in GDP (WDR 2016: 3).

Since 2000, there has been a considerable increase in connectivity, creating new tools for economic and social development – and there is no reason to believe that this trend will not continue. The UN (2015: 7) has estimated that the number of mobile phone subscriptions had increased from 2.2 billion in 2005 to 7.1 billion by 2015. Furthermore, 3.2 billion people (of whom 2 billion are from developing countries) are expected to have online access by the end of 2015. These technologies are being adopted at such a speed that they are reaching many of those who remain below the poverty threshold. For these people, ICT represent an entry ticket to formal networks to communicate, to transact and access basic financial services, to obtain information, and to demand their rights and recognition. In January 2016, the World Bank issued its annual world development report, devoted in its entirety to digitalization and development, and focusing on unrealized digital dividends. Concurring with UN estimates, the World Bank also highlighted the number of people still untouched by the digital revolution:

> Only around 15 percent can afford access to broadband Internet. Mobile phones, reaching almost four-fifths of the world's people, provide the main form of Internet access in developing countries. But even then, nearly 2 billion people do not own a mobile phone, and nearly 60 percent of the world's population has no access to the Internet. The world's offline population is mainly in India and China, but more than 120 million people are still offline in North America (...) In Africa, the digital divide across demographic groups remains considerable. Women are less likely than men to use or own digital technologies. Gaps are even larger between youth (20 percent) and those more than 45 years old (8 percent). (World Bank 2016: 6–7).

Connections have been made between the WSIS+10 and the UN SDGs, such as action lines for achieving these goals through ICT.[4] These initiatives, together with the World Bank report, have drawn considerable international attention to this agenda, and ICT is increasingly and rapidly becoming a precondition for sustainable development. Carl Bildt, former prime minister and foreign minister of Sweden, is among those who have argued that information technology has the potential to become the most important tool for development to billions of people living in Africa and Asia (Bildt 2015). In policy circles and documents concerned with development politics, these technologies are increasingly becoming a core focus of development strategies. However, unless accompanied by a focus on cyber security, development will be hollow and thereby unsustainable.

Donor countries and international organizations seize on digitalization as an opportunity for fighting poverty. However, digitalization in countries that suffer from lack of development, poor governance and poverty may provide new breeding grounds for organized crime, terrorism, and cyber security challenges. Thus, a new dimension of social vulnerability follows in the wake of the development opportunities offered by the digital revolution. Baseline studies have demonstrated the gap between the development goals and intentions in donor policies, and digital vulnerability and cyber security in developing countries.[5] In order to be sustainable, digital development must be followed up by a focus on digital security.

This can be accomplished through core development and aid activities, and projects focused on improving the analogue foundations for digital technology, including knowledge, information, education, employment and institutions.

4 See: https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_booklet.pdf and http://workspace.unpan.org/sites/Internet/Documents/UNPAN95707.pdf in particular bulletpoint 4.

5 Myanmar: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Myanmar.pdf
Tanzania: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Tanzania.pdf

Digital dividends in developing countries

In 2015 the World Bank published its new global poverty estimates, confirming that the target of halving the rate of extreme poverty was achieved seven years ahead of schedule. The new goal of eradicating extreme poverty in the course of the next 15 years has now been endorsed by the UN through the SDGs. Some claim that it will be possible to achieve this, because the developing world is fundamentally changing thanks to the connectivity made possible by digital networks. However, even though the digitalization of developing countries is spreading rapidly, achieving faster growth, more jobs, better services and the broader benefits is likely to be more difficult (World Bank 2016).

In the following, I group the challenges that obstruct the realization of digital dividends in developing countries under two headings i) weak technological environment, ii) poor network infrastructure and urban-centred digitalization.

i) Weak technological environment

The need to build the correct environment for technology before businesses can begin to thrive and then reap the benefits of digital connectivity has been emphasized by international organizations and policymakers (see for instance ITU 2012, WDR 2016). Research has pointed in the similar direction, like the study by Klimburg and Zylberberg (2015) and the Dalberg Report (2013) Based on a survey of more than 1300 businesses, 1000 small and medium-sized enterprises and extensive interviews in Ghana, Kenya, Nigeria and Senegal, the Dalberg Report maps the impact of the Internet as a force for growth and social change. It describes the digitalization of these countries as a work in progress, with the potential still largely untapped. Further, the Dalberg Report calls for more and better information that can guide policymakers and investors in capitalizing on this potential, and stresses that countries will need to invest in infrastructure and the broader ecosystem for innovation. It further identifies 'core infrastructure' and 'conditions for usage' as the two key pillars for a well-functioning Internet economy (2013: 9). The Dalberg Report highlights how core infrastructure requires an environment not just with mobile and Internet access, but also with electricity, skills, knowledge, education and awareness of corruption. Establishing such an environment is dependent of a set of conditions for usage such as costs, education, and relevance of services. These conditions are in turn influenced by degree of access, relevance, availability and attractiveness. In other words, digital dividends need to be built on analogue

foundations. Core traditional development politics and projects become central elements for bridging the digital divide.

In order to illustrate and contextualize the importance of this aspect, let me offer a few empirical snapshots from developing countries currently experiencing rapid digitalization.

Botswana has one of the highest percentages of Internet subscribers on the African continent. The digitalization of Botswana has mushroomed: there have been substantial investments in digital infrastructure; the country scores high on Internet usage; Botswana has a national policy on Internet distribution and access points (including rural areas), and the highest percentage of social media users on the sub-Saharan mainland. Such statistics would indicate that Botswana has indeed become an Internet society – but, looking beyond these figures and studying the actual impact of digitalization on people's everyday lives, the picture is rather different. Examining Botswana's two major industries – diamonds and cattle farming – the anthropologist Jo Helle-Valle demonstrates the relevance, or lack of relevance, of digital technology and the Internet in the lives of ordinary people (2015). The diamond industry is global and very much controlled by foreign capital, and through these connections the industry might be said to be fully digitalized. However, as Helle-Valle notes: '... the Botswana work-force in this sector is typically manual labour, with little or no digital technological competence being required' (2015: 3). In this important sector Botswana is not very digitalized, nor is there perceived to be any great need for this.

The situation in the cattle industry is very different. Helle-Valle shows how broad and innovative ICT projects have led to effective management of the national stock and a thriving export industry. Thanks to new technology, most of the cattle in Botswana are now included in a system which, by means of digital chips in each animal, can monitor and identify sickness, ownership, breed, theft, etc. The data can be read through handheld devices such as smartphones, tablets or computers, and are loaded into large databases. (Helle-Valle 2015: 3). Through this system, cattle owners can communicate more easily with veterinaries as well as buyers and sellers.

Digital technology has also been used in Africa to strengthen internal solidarity and economic growth. In Kenya, fundraising campaigns through mobile phones and social media have raised considerable amounts of money for famine relief in the northeast of the country. In 2007, the telecom company Safricom launched a mobile money service called M-PESA which attracted six million customers within two years, transferring billions annually. Through M-PESA, people without bank accounts could leapfrog from traditional brick-and-mortar finance to digital economy (Mbogo 2010, Bright and Hruby 2015). The launch of M-PESA sparked a series of digital innovations in the country. Ushahidi,

an app for digitally and rapidly reporting and tracking outbreaks of violence in connection with elections, was also launched in 2007; in the following year it became an international tech company based in Ngong Road, or what has become known as the Silicon Savannah, the tech-hub of East Africa. In 2011, the Kenyan Red Cross together with Safaricom led the *Kenyans for Kenya* campaign, raising almost 12 million dollars in four weeks for aid during a severe famine. The social media were also used to inform and coordinate help during the Westgate crisis, and the Kenyan Red Cross employed the social media to get blood donors following the attack (Were: 2013). A few years earlier such mobilization would not have been possible.

Another country that is now surfing the digital wave is Rwanda. Considerable investments have been made in ICT technology in schools as well as in infrastructure, aiming to '... strengthen skills training centres and develop an ICT culture in schools as a means of creating a critical mass of IT professionals' (Tafirenyika 2011). Furthermore, together with the Rwandan government, the Kigali Bus Service has invested in a cashless, card-based public transport ticketing system known as *twende.* By 2015, more than 30,000 customers had signed up for this system. This initiative was part of the government's Smart Kigali programme for rapid modernization and digitalization of the capital city (Dusabirane 2015).

While the digital dividends in the cattle industry in Botswana, in the social media campaigns in Kenya and the digitalization programmes in Rwanda are evident, there are still many hurdles to be dealt with before most people in these countries can enjoy extensive use of the Internet, the most important hurdle being economic. Although the importance of being connected is recognized, the consumer costs are still too high for most people to be able to afford to use the social media and the Internet on a daily basis. The World Bank also highlights this aspect, and how the bottom billion are reaping only a modest share of the digital dividends:

> In the Central African Republic, one month of internet access costs more than 1.5 times the annual per capita income. Even mobile phones are expensive: the median mobile phone owner in Africa spends over 13 percent of her monthly income on phone calls and texting. And many poor lack the basic literacy and numeracy skills needed to use the internet. (World Bank 2016: 16)

The digital gap is closely linked to the economic gap: the 'haves' can make use of the new technology and reap digital dividends, while the 'have-nots' are left behind. This is where development efforts can make

a difference. By helping to bridge this infrastructural gap, donor countries can play a key role in contributing to improve the technological business environment in developing countries.[6]

ii) Poor network and infrastructure – urban-centred digitalization

In measuring the availability, accessibility and affordability of digital network and infrastructure, the World Bank has divided this infrastructure into three miles: i) the first mile is where the Internet enters a country, ii) the middle mile is where the Internet spread through the country, and iii) the last mile is the level where the Internet actually reaches the end users. Additionally, the invisible mile, which concerns important but less visible elements necessary for maintaining the integrity of the three levels of the infrastructure, is often included in this division of infrastructure (World Bank 2016: 205).

Much has been done in African countries in order to improve the first mile and the international gateway, the point where countries connect to the global Internet. Since 2009, thousands of kilometres of undersea broadband cables along the coasts of East Africa (see e.g. SEACOM) and West Africa (see e.g. WACS) have been bringing faster Internet to the continent. These cables provide countries such as Djibouti, Ghana, Ivory Coast, Kenya, Madagascar, Mozambique, Nigeria, Senegal, South Africa, Sudan and Tanzania, and with high-speed Internet. While governments can negotiate higher Internet speed, better prices and greater bandwidth, user conditions and Internet accessibility/availability are very much conditioned by the middle mile, the national backbone and intercity networks. These, in turn, depend on the degree of competition between public and private actors in the country. The rules of the market competition vary from one country to another, and affect the user side of digital networks and infrastructure. Liberalizing the market for the middle mile is an effective way of providing open access and Internet to end users – but, as the World Bank has pointed out, this entails a risk '... that the most popular routes – say, between the two main cities – are 'superserved' while the rest of the country is underserved.' (2016: 219)

In developing countries, the last mile is rarely served through fixed copper cables, as local access to networks is dominated by wireless alternatives. This is where the digitalization trajectory of developing countries differs the most from developed countries, due largely to the problem of the fixed vs wireless networks. Whereas the developed countries

6 Various methodological models for fostering more efficient cyber security capacity building have been developed; for an overview see Klimburg and Zylberberg 2015: 20–26, and Muller 2015.

had achieved almost universal fixed-line access before wireless technology took over around 2001, most developing countries never built fixed-line networks. The World Bank sees this point as important

> ... because wireless networks [...] are not fully substitutable for fixed networks [...] either in usage (which rarely offers flat-rate pricing, without data limits) or in performance (where speeds are generally lower) [...] many developing countries are stuck with a second-class internet that may fail to deliver the expected benefits, especially for business users. (2016: 208)

The 2016 World Bank report goes on to describe how developing countries will have to struggle to achieve a fully and sufficient middle mile or national backbone. Some developing countries may achieve such a backbone through private–public partnership, but creating fixed-line networks in rural areas is still challenging and not very likely. Moreover, according to the report, fragile countries such as DR Congo and South Sudan are unlikely to ever get fixed-line access, even in urban areas. Klimburg and Zylberberg (2015: 9) note the importance of internet availability and an adequate backbone network infrastructure, network ownership and geographic patterns of network development as key for better business environments and improved digital dividends. Furthermore, they claim that this situation creates '... few incentives for local actors to either build network capacity in mostly rural areas or to expand network coverage. Development efforts need to focus on bridging this infrastructural gap, as a key determinant in an enabling business environment' (ibid.). Other countries, such as Botswana, Burkina Faso, the Central African Republic, the Democratic Republic of Congo, Gabon, Kenya, Rwanda Swaziland, Tanzania and Togo completely lacked the last mile (WDR 2016: 255). In these countries analogue foundations for digital enterprises are weak, and there are no incentives for digital companies, such as online retailers. Unless global development initiatives intervene, these developments point towards a trajectory of urban-centred digitalization in the developing world, with new kinds of societal vulnerabilities.

Developing countries and new kinds of societal vulnerabilities

ICT has become a highly important foundation for most infrastructures in developed societies, and the developing countries are now following in their path. Individuals, businesses and nations are depending more and more on data and systems in the virtual world. In this global transition into the digital era it is easy to forget that the Internet was not invented for carrying the critical features and infrastructure that it does today, including key societal sectors such as energy, power, economy, health, communications and transport. The increasing interconnectedness of these features implies a major change in the societal risk factors facing us today, and also highlights the tight linkages between the domestic and international dimensions of politics. Global, complex and rapidly shifting trends impinge on domestic political contexts, especially along the security dimension. Along with the opportunities and possibilities shaped by the digital revolution come new, more transnational challenges to major areas of societal infrastructural as well as industry, innovation and business. These threats cannot be reduced to technological concerns, as they are interconnected with international politics and global trends. Fragile states with poor infrastructure and governance are rapidly being connected to the Internet – but the digitalization of these countries is hollow. This hollowness can provide room for cyberspace actors with bad intentions that will affect not only domestic problems in developing countries and fragile states, but global society as well.

Although developing countries are following in the path of developed countries and becoming more digitalized, they are taking a different route. For the developed countries, digitalization has been a long-term sequential evolution: initially based on state-led investments in fixed telephone infrastructure, it was followed by private initiatives and innovations, and then, building on this infrastructure established gradually over more than a hundred years, came the addition of mobile phones, smartphones and the Internet. Developing countries, by contrast, are leapfrogging straight into wireless technology and mobile and internet networks that are often built by the private sector (which obviates the need for investments in wiring with expensive copper cables). Jumping into the digital age has provided developing countries with digital technology, new opportunities and better connectedness. But the introduction of technology in these societies has been proceeding far more rapidly than the building of state institutions and other mechanisms that can manage new challenges arising from this technology. Digital technologies are being put to use before good, functional regulatory mechanisms have been developed and put in place. The resultant shortcomings

– in state mechanisms, institutions, coordination mechanisms, private mechanisms, general awareness, public knowledge and skills – open the way to new kinds of vulnerabilities.

Developing countries become digitalized rapidly, but they are weak in the knowhow, awareness, institutions and skills needed for dealing with cyber security issues. This vulnerability can be met through development assistance from donor countries to projects and activities focusing on awareness, knowledge, information, education and employment. In this context, Cyber Security Capacity Building (CCB) becomes integral to development.[7] Linking CCB to the SDGs can strengthen the sustainability aspect of these goals. Moreover, the dissemination of accurate information regarding security and structural aspects of the Internet is likely to make developing countries more competent actors on the global arena where international cyber politics is developed, and thus better positioned to exert influence on their own position in the future.

Box 1. From an interview with Hans Christian Pretorius (Head of department at the Norwegian National Security Authority (NSM))

Because of the borderless nature of cyberspace, many have held that risks are not confined to countries and regions. This indicates that cyber security is only as strong as the weakest link, which in turn implies that weak cyber security in one country negatively affects global cyber security. Following this logic, enhancing cyber security in one place will benefit the larger system and the international community at large. However, this theory is contested, and we at the NSM do not consider fragile states with weak institutions a direct threat to Norwegian cyber security in this manner. Nevertheless, Norway should be doing cyber security capacity building in developing countries and fragile states – but, instead of being motivated by the need to enhance Norwegian cyber security by securing the weakest link, this should be motivated by more traditional Norwegian developmental concerns. In order to combat poverty and ensure regional stability, cyber security needs to be an integral part of development.

In our view, among the security challenges for developing countries embracing the digital revolution is the global trend towards buying better cyber security from private companies. Furthermore, national cyber policy usually does not affect the private sector in particular – on the contrary, there are often conflicting concerns between commercial interests and security interests. Private companies are free to decide how much risk they want to take, and expensive cyber security measures may not always be prioritized in developing countries. This can contribute to further hollowing the digitalization of developing countries, expanding the digital divide between developed and developing countries. This challenge could be confronted if developing countries' cyber security capacity building strategies were followed up by implementation and legislative changes. Because digitalization is primarily driven by commercial interests, this also calls for increased public–private cooperation in the development sector. Additionally, developing countries should be trained in gearing themselves to become part of the international CERT (Computer Emergency Response Team) cooperation, and Norway could help facilitate such teams through capacity building and lifting the knowledge and expertise in developing countries about CERTs.

7 See also Pawlak 2014.

The Security/Development nexus

Drawing on the scholarly tradition on the security/development nexus, Klimburg and Zylberberg (2015) identify CCB as a key component of development. They hold that this combination is particularly important because:

> ... the areas with the highest potential of economic growth correspond roughly with those where the security risks are the highest [and] the skills developed locally through cyber security trainings correspond to those needed to enable local businesses to scale up, without having to rely on outside, more expensive talent. (Klimburg and Zylberberg 2015: 10)

CCB generally includes three categories: technological, human and organizational resources. Although helping to provide access to information and communication technology is seen as an important part of the development agenda (WDR 2016), it is the building of institutional and human resources that should be the main priorities of donor countries' development politics.

Botswana, Kenya, Mozambique, Myanmar, Rwanda and Tanzania are developing countries experiencing a rapid growth of digitalization and digital connectivity. This connectivity fuels a fundamental transformation in these countries' social, political and economic spheres, changing people's everyday lives. The up-side of this digital revolution is that it can help people out of poverty, and turn the economies in some African countries into some of the fastest growing in the world. When entrepreneurs, farmers or fishermen can receive and transfer money digitally through the Internet it becomes easier and safer to run small and medium-sized businesses. Connectivity also makes it possible to compare prices and different markets, which farmers, fishermen as well as small and medium-sized businesses can put to good use.

However, along with the up-sides come some down-sides. The digital trajectories of developing countries involve a different set of cyber threats than those in the developed world (Subrahmanian et al. 2015). Nir Kshetri has described the digitalization of the Global South as characterized by a certain *hollowness* (2013: 153), involving different things for different entities. For instance, it may refer to weak institutions, poor organizational and individual defence mechanisms, better recruitment basis due to high unemployment and low wages, and a lack of capacity to manage risks and vulnerabilities in society (Kshetri 2010: 1057). Botherders[8] and other cyber criminals tend to come from locations where

8 A botnet consists of many internet-connected computers where components communicate and coordinate actions that can be used to send spam email of ddos (distriuted denial-of-service) attacks (Coleman 2015: 93). A bot herder or a botnet herder is a person who controls and maintains a botnet by installing malicious software in numerous machines, putting these machines into his or her control. These machines can then be used to attack or infect other machines.

high-paying IT jobs are rare or unavailable (Sullivan 2007); and in developing countries the growth of IT jobs is lower than the growth of Internet penetration (Kshetri 2010: 1071).

The lack of capacity can be due to technological, behavioural and policy-related factors. Generating innovation, primarily driven by commercial forces, without attention to security has left a digital hollowness in these developing countries which makes it easy to target unprotected devices and unskilled users which in turn makes these countries attractive for cyber criminals. Developing countries also lack the resources to build institutions to combat transnational crime (Cuellar 2004). Laws that recognize cyber crime, law enforcement mechanisms, personnel who understand cyber crime, as well as the awareness necessary for dealing with cyber crime – all these remain inadequate. Given their weak institutions, limited capacity, and generally low resources for fighting cyber crime, these countries are likely to remain attractive for cyber-criminals also in the future.

Without attentions to analogue foundations, there is a risk that this hollowness will escalate when developing countries invest in more sophisticated ICT technology and digital connectivity. In addition to investments in security measures such as anti-virus programmes, there is also a need to improve basic knowledge about ICT. Poor and fragile institutions in many developing countries have contributed to this digital hollowness. Franz-Stefan Gady, a senior fellow at the EastWest Institute and founding member of the Worldwide Cyber Security Initiative, has noted the statistics on the high numbers of PCs infected with viruses and malware in Africa and how these computers are easy targets for botnet operators (2010). Several experts have pointed out how rogue states and developing countries become hosts to outlaw servers, also called bullet-proof hosting. The hosts of these servers operate beyond the reach of most law enforcers and enable cyber crime elsewhere (Palmer 2016, Goncharov 2015). Others have highlighted how certain vulnerabilities in the global network such as on the SS7 (the network that allows cellular carriers to route calls, text and other services to each other), which was built in the 1980ies, can be used by people with illicit intentions for surveillance and may undermine the privacy of cellular customers (Landau 2010). Through the SS7 "... a single carrier in Congo or Kazakhstan [...] could be used to hack into cellular networks in the United States, Europe or anywhere else." (Timberg 2014).

In 2011 Immacuate Karambu pointed out that little was being spent on cyber security, also in the financial sector. In 2011 only 40% of banks in Kenya, Uganda and Tanzania were prepared against cyber threats (Kshetri 2013: 159). Weak institutions and law enforcement mechanisms on cyber crime contribute further to the digital hollowness of developing countries. Digitalization can be a key factor for economic and social development, and even democratization, but such a development also opens new frontiers for criminals and others with bad intentions. As

Langø has argued: 'ICT can potentially be either a boon or a threat to democracy: it can aid peaceful opposition or violent rebellion; help governments enforce the rule of law or repress the population.' (2016: 5). Policymakers concerned with building cyber security capacity should take such threats and risks into account when engaging in developing countries. The prior analogue foundations in a country very often determine the direction of the digitalization.[9]

Box 2. Interview with Telenor Group

Telenor is among the major mobile operators in the world, with more than 200 million mobile subscriptions, and is present in markets with 1.3 billion people. Several of these are developing countries. Telenor has an ambition to connect 200 million people to the Internet by 2017 facilitating access to knowledge, opportunities and vital services also in developing countries.

Among the challenges in connecting developing countries to wireless communication technology are those pertaining to lawful interception, authority requests, surveillance and privacy. Awareness-building information campaigns and gatherings with constellations of authorities, local authorities, international organizations, national organizations, NGOs, private actors, senior networks and women's networks may considerably improve the cyber security level within a country. The awareness dimension and the facilitation of various niche capabilities like CERTs and institution building are also areas where Norwegian expertise could be exported and contribute to counteracting the hollow digitalization of developing countries.

Not only within the individual developing country, but also in the region and furthermore as host for malicious activities, CCB in these developing countries can ultimately impact on the security of donor countries as well. In order for economic and social development to be sustainable, and in order to achieve the goals of the international community to combat poverty and inequality by 2030, cyber security must be recognized as a key element; and needs assessments of developing countries' cyber security maturity should be included as an important mapping activity towards achieving these goals.[10]

Digital hollowness must be addressed comprehensively, and cyber/capacity needs should be understood and contextualized in connection with core conditions for economic and social growth in developing countries. This includes the rule of law, education, programmes to promote small and medium-sized businesses, as well as donor programmes facilitating participation of developing countries (civil society

9 See for instance Wagley 2014, and Langø 2016: 18–19.

10 For an overview of different models measuring cyber capacity maturity in developing countries see Muller 2015: 7–10.

and governments) in the multi-stakeholder approach to Internet governance.

Box 3. From an interview with Margrete Raaum (FIRST Norway)

FIRST (Forum of Incident Response and Security Teams) is an international confederation of trusted computer incident response teams. FIRST was established in 1990, one year after the CERT Coordination Center was created. As of 2016, FIRST has 345 teams in 74 countries. These teams cooperatively handle computer security incidents and offer education/training programmes and fellowships to developing countries. The fellowships are established to build capacities in developing countries so that they can match FIRST's requirements for joining the training programmes. FIRST has a limited number of Fellowships, but is open to partnering with organizations that are willing to contribute to the fellowship programme. In this way there is an opening for MfAs, or other sponsors, to strategically sponsor such fellowships in developing countries on their focus lists. The fellowship programme stretches over a period of five years.

Through FIRST programmes, local activities pertaining to cyber security in developing countries are facilitated and built upon. FIRST can arrange small-scale conferences in developing countries that are already on FIRST programmes, in a fellowship, or seek to join the programme, such as Botswana, Uganda, Ghana, Mauritius and Tanzania, as well as several countries in South America. In these conferences FIRST typically collaborates with local organizations and provides trainers and education.

The training programmes are focused on teaching how CERTs can be established, what requirements and conditions must be met in order to establish a CERT, and what kinds of functions the CERTs are intended to have. Through the training programmes, FIRST offers a CERT start-up kit to developing countries that match FIRST's list of requirements. The programme runs for a three-year period.

FIRST feel that the rapid digitalization of developing countries is not being followed up with security measures. This leads to new kinds of security concerns pertaining to, for instance, the financial sector and the energy sector in these countries. Therefore, many developing countries are eager to establish government CERTs in order to protect the government from cyber threats. Furthermore, through their CERTs, developing countries may gain a point of contact for international cooperation on cyber security issues. In this way CERTs also contribute to making developing countries more visible and involved in international cyber -security processes.

From the perspective of FIRST Norway, building cyber security capacity should focus on establishing CERTs and protect governments from cyber threats, but also on protecting critical infrastructure.

International cyber politics and developing countries as potential swing-states

Inter-country exchange of information and experience gained is an important element in producing and developing new international cyber politics. Because of the rapid development of ICT, and the even more rapid pace of connectivity across the globe, old political challenges in international relations resurface in new and sometimes unexpected ways. In this political landscape there is a dire need for new norms, policies and trust. The multi-stakeholder approach, hailed as a way forward in international relations concerned with cyberspace, involves states, international organizations, private actors, think-tanks and NGOs. In this way, cyberspace as a political topic in international relations incorporates new kinds of partnerships. There has been considerable research on international relations, global governance and international organization, but only a marginal part of this work has been engaged with cyberspace and how it is changing well-established patterns in international relations. While international bodies like the UN, EU and NATO are important players in developing international cyberspace policy, they are not able to fully incorporate the multi-stakeholder approach involving, for instance, big private enterprises like Google, Facebook or Huawei. On the other hand, as long as the technological revolution is run by the private sector, these actors have no formal say in international organizations such as the UN.[11] Thus while maintaining its focus and prioritized collaboration with international organizations (the UN, EU, NATO, AU, etc.) Norway should also seek ways of working together with major private enterprises, perhaps especially in connection with development and aid.

Another challenge is that many governments in the developing world lack the knowledge, awareness and mature policies about cyberspace and cyber security necessary for participating fully in the global arena. In this context there are potentials for donor countries to incorporate CCB into their more traditional focus on development concerned with institution building, cooperating with states, civil society and NGOs, developing various kinds of partnerships. Embarking on such programmes can contribute to new partnerships, and sustainable development with

11 The multi-stakeholder process seems to be gaining a footing also in international bodies like the UN. Although the majority of those speaking at the December 2015 WSIS+10 meeting at the UN General Assembly were state representatives, it should be noted that spokespersons from several private companies also took the floor.

social and economic growth, as well as giving donor countries an advantage in the global arena of international cyber policy. As pointed out in a recent NUPI report, the dichotomous character of current international cyber policy on how Internet should be governed implies that '... the importance of the 'swing-states' – nearly all within the developing world – rises' (Klimburg and Zylberberg: 2015: 46). Collaboration among academic institutions, national and international organizational, and decisionmakers from donor and recipient countries seems the most natural way to explore these links and to identify potential CCB programmes for development policy where such partnerships can be built.

Development, local ownership and cyber space

Most donor-driven development assistance is in one way or another concerned with the 'ownership debate'. Although not yet very prominent in policy documents, this debate is also relevant for CCB projects. The term 'ownership' has a long trajectory in development traditions and needs further clarification here, in order to connect it to CCB.

In development work, the term *local ownership* emerged in the report of the OECD's Development Assistance Committee (DAC) in 1996. This document highlighted the importance of locally owned development strategies, defining local people in their relation to donors. Such ownership built on an idea that had featured within the development sphere for some time: that aid would be more effective if the recipients could control how it was being used. This view has since been adopted by the World Bank, the OECD, the UNDP, and a great many NGOs. Local ownership was one of the principles of the 2005 Paris Declaration on aid effectiveness, later followed up in Accra (2008) and Busan (2011).

The debate on ownership has also been an important one in international peacebuilding and statebuilding engagements. In peacebuilding the role of local and national ownership in maintaining the legitimacy of the activities is highlighted:

> Effective approaches to national and local ownership not only reinforce the perceived legitimacy [...] and support mandate implementation, they also help to ensure the sustainability of any national capacity. (UN DPKO/DFS 2008: 39)

The UN further highlights that a precondition for national and local ownership is a strong understanding of the national political and wider socio-economic context (ibid.). Donors see local ownership as critical for the successful *implementation*, *legitimacy* and *sustainability* of development projects. According to UN and World Bank policy documents, the primary way of doing this is through dialogue, but also: 'Political, financial and other forms of international leverage may be required to influence the parties on specific issues, but those should only be used in support of the wider aspirations' (UN DPKO/DFS 2008: 41).

The concept of 'ownership' has remained vague. It is used to refer to several different things, and there seems to be a tension between theory and practice. As employed in the Paris Declaration, the term can refer to control over decisions, development policies, strategies and coordination of development actions (de Renzio, Whitfield & Bergamaschi 2008).

But it may also refer to commitment to a set of policies, regardless of the process and actors behind the making of these policies (ibid.). As Axel Borchgrevink, an anthropologist who focuses on development studies, has pointed out,

> ... the crucial issue is really if the recipient government is committed to a certain policy *as if it is their own*, not whether they have come up with on their own. In this perspective, the heart of the matter is therefore the commitment to the policy, while the issue of who makes the decisions fades into the background. (Borchgrevink 2012: 17)

Two opposing views on development have emerged: (i) that development is an activity where the international community increasingly seeks to equip developing countries with 'ownership' of their own country's politics and policies, and (ii) that the only thing developing countries get 'equipped with' through development projects is ownership of an existing or given rationality of governing. It is symptomatic of this second view that the situational analyses conducted by international organizations like the World Bank and the UN assess all countries according to the same criteria – which, however, presupposes the existence of an ideal policy, regardless of the specific context.

This is also a challenge with most projects for building cyber security capacity. There are many different actors and approaches to CCB – here let me mention the Cyber Index of the UN Institute for Disarmament Research, the Belfer Center at Harvard and its *Cyber Readiness Index 1.0,* the Australian Strategic Policy Institute's *International Cyber Policy Center Maturity Metric*, the Asia Pacific CERT network's *Cyber Green*, Microsoft's *Linking Cyber security Policy and Performance,* and the *Cyber Security Capability Maturity Model* at the Global Cyber Security Capacity Centre at Oxford.[12] However, all these approaches are embedded in normative approaches that apply and promote certain sets of values, ideas and standards, ranking them according to a universalistic teleological view on world history. As also Francis Fukuyama (2014) has noted, transferring modern institutions to developing countries or other societies can succeed only as if the transfer is anchored in these countries' own context as regards existing rules and the political forces supporting these rules. This in turn means that the evaluations offered by various CCB needs assessments would benefit from being contextualized, rich and detailed in their descriptions, and incorporating knowledge based on empirical research. This work should be carried out as most traditional development projects have done, including infrastructure development (*first mile*, *middle mile*, *last mile* and *invisible mile* (World Bank 2016: 205)), with attention to rule-of-law aspects and the broader economic and social factors.

12 For further details about the various approaches see Muller (2015).

The ownership debate has long traditions in the development literature, but very few have examined ownership and how it pertains to CCB. Because of the role assumed by the private sector in the digital revolution, the public–private relationship in this field should be viewed also in terms of 'ownership'.

Ownership and public–private cooperation

Most of the world's critical cyber assets are owned and managed by private enterprises. This means that states are dependent on private companies in order to provide public security. And yet, states seem to be very protective of their own power and authority involving cyber security. Where cyberspace used to be dominated and produced by private actors, states are now increasingly entering the field of cyberspace and enforcing state authority. It is important to explore this tendency, paying attention to the ownership debate in development and peacebuilding studies. As noted, cyber security involves a multitude of actors both inside and outside of governments, with differing representations and concepts of security – political, social, economic, corporate and private. In this context, where ideas of security (whose and what) can become contested and politicized, research is needed to underpin policy recommendations and ideas of ownership:

> Cyber security research is steadily growing, but in international relations and security studies, it is not a mature field yet. Apart from a few exceptions, research remains fragmented, is biased towards just one expression (cyber war), and struggles to tap into existing funding resources. Given this relative weakness, many important issues remain under-researched. The importance of 'the private' in the establishment of the topic as national security issue is one of those issues (Cavelty, forthcoming 2016: 14).

Cyber security differs from other security areas in one key way: traditionally it has been private actors who have been entering into state security domains, but with cyber security it is the other way around. States are now trying to (re)establish, take ownership and gain terrain in cyberspace, a space which has been cultivated by innovative companies and consumers – but also by criminal elements. For donor countries engaged with aid and development in developing countries this represents a challenge, because many of the structural assumptions about ownership, authority and governance previously taken for granted must now be questioned.

This will require mapping such structural challenges and identifying potentials for public/private cooperation in development engagements in developing countries. Topics that could be explored for potential donor involvement concerning ownership include social responsibility and

cyber security, lawful intercept and authority requests, security and privacy, public awareness, ethical challenges, and possible constellations with governments, private actors and NGOs.

Conclusions

This report has shown how digitalization and cyber security as new global challenges are becoming increasingly central to the organization of development assistance – with consequences for billions of people in the developing world. With the emergence of digitalization and cyber security challenges, the transfer of knowledge and experience from traditional donor countries to the developing countries becomes crucial, perhaps even more important, than the transfer of funding. In the long term, this development may contribute to more equal partnerships, in which the interests of donors as well as of recipient countries are safeguarded. This report has also shown how new development actors (public and private) are becoming involved, making the group of donors more diverse and bringing in different policy traditions and ways of thinking. Drawing on the old adage '*Give a man a fish and you feed him for a day; teach a man to fish and you feed him for a lifetime'*, the title of this report points to the importance of sustainability through teaching and educating people in developing countries about digital skills and opportunities. However, in the same way as teaching someone how to surf ocean waves is not enough in order to master those waves, teaching someone how to surf the Internet is not enough to bridge the digital divide. Surfers need surfboards, but they must also know how to swim, must understand the forces of the waves, and be familiar with the local context, currents, corals and reefs below the surface. Merely teaching someone how to surf the Internet is not enough to foster sustainable development. Access to the Internet must be combined with analogue foundations, knowledge, awareness and a digital environment where the focus on security will be increasingly important.

There are in cyber space many *corals*, *reefs* and *currents* that must be understood. The research reviewed here indicates that there are opportunities for donor countries in this field. Digitalization brings with it a pressing need for knowledge, education, institution building and experience-sharing among countries and regions. Although traditional development mechanisms can be applied to enhance sustainable development through building cyber security capacity, this combination also introduces new aspects and dilemmas in the field of development. Private actors have dominated the trajectory of the digital revolution. The digital environment, or cyberspace, has been fostered and developed by companies and consumers – and also by less honourable actors. This trajectory has produced a set-up in which private actors have assumed the dominant role. For development actors, this represents a challenge, because many of the structural assumptions about ownership, authority and governance that have underpinned traditional development policies are now turned upside-down.

As shown in this report, building cyber-security capacity in developing countries must be conducted on several levels, simultaneously, through a holistic approach. There are the technological, organizational and human dimensions, and the local, national and international levels. Norway has long traditions of successful international engagement in working on all these levels, and the importance of exchanging knowledge, lessons learnt and building trust between countries has often been emphasized. Building capacity in cyber security represents a relatively new political field, not properly included in the UN's SDG (2015) or even in the World Bank's *World Development Report – Digital Dividends* (2016), where donor countries like Norway can continue their long-term foreign policy traditions by incorporating a new policy field. Distinct properties of cyberspace – such as the fact that it has no borders, few rules and free flow of information – trigger new kinds of challenges with regard to international politics and diplomacy. Managing such challenges will require in-depth understanding of the democratic, social and economic development contexts on which cyberspace depends.

Recommendations

- Baseline studies show that there is a gap between development goals and intentions in donor policies, and the level of digital vulnerability and cyber security in developing countries. This indicates that, if digital development is to be sustainable, it will need to be followed up by a focus on digital security. Here donor countries can assist, through core development and aid activities, with projects focused on improving the analogue foundations for the digital technology such as knowledge, information, education, employment and institutions – but also by facilitating arenas where experience and lessons learnt can be shared at local, national and regional levels.

- Norway has a long track record of development assistance as well as with multilateral diplomacy. Combining these two dimensions, through cyber security capacity building (CCB), could provide excellent opportunities for Norwegian foreign policy to strengthen Norwegian long-term interests like the production of new norms, as well as following up on the SDG commitments by contributing to the digital revolution in developing countries.

- Because digitalization has been driven primarily by commercial interests, greater public–private cooperation is necessary in the development sector.

- Developing countries should be trained in how to gear themselves to become part of the international CERT cooperation. Donor countries like Norway could help to facilitate this through capacity building, collaborating with actors such as FIRST, and by improving knowledge and expertise in developing countries about CERTs.

- FIRST has a limited number of Fellowships, and seeks to partner with organizations willing to contribute to the fellowship programme. Here is an opening for ministries of foreign affairs, or other sponsors, to strategically sponsor such fellowships in developing countries on their focus lists.

- While maintaining its focus and prioritized collaboration with international organizations such as the UN, EU, NATO and AU, Norway should also seek ways of working together with major private enterprises, perhaps especially when engaging in development and aid.

- Awareness-raising information campaigns and gatherings with constellations of authorities, local authorities, international organizations, national organizations, NGOs, private actors, senior networks and women networks may considerably improve the level of cyber security level within a country. The awareness dimension and the facilitation of various niche capabilities and institution-building are also areas where Norwegian expertise could be exported, to help in counteracting the hollow digitization of developing countries.

- To this end, Norway could for instance export the concept of Nasjonale sikkerhetsmåned (National security month) focusing on cyber security. Other potential niche capabilities for export through development activities include nettvett.no slettmeg.no and Security Divas – the latter in particular would readily fit with Norway's traditions of enhancing and strengthening women's rights and security in developing countries.

Literature

Bildt, Carl. 2015. 'Development's digital divide', *Project Syndicate,* available at: http://www.project-syndicate.org/commentary/sustainable-development-goals-digital-divide-by-carl-bildt-2015-08 (accessed 29.02.16).

Borchgrevink, Axel. 2012. 'Midnight in Paris: Nicaragua, aid donors and notions of ownership', paper presented at the panel 'Development and Ethnography of Aid Partnership,' at the annual conference of the American Anthropological Association, San Francisco, 13–18 November.

Bright, Jake and Aubrey Hruby. 2015. 'The rise of Silicon Savannah and Africa's tech movement', *Tech Crunch,* available at: http://techcrunch.com/2015/07/23/the-rise-of-silicon-savannah-and-africas-tech-movement/

Cavelty, Myriam Dunn. Forthcoming 2016. 'Cyber-security and private actors', in *The Routledge Handbook of Private Security Studies*. New York: Routledge.

Coleman, Gabriella. 2015 *Hacker, Hoaxer, Whistleblower, Spy – The Many Faces of Anonymous*. New York: Verso.

Cuellar, Mariano-Florentino. 2004. 'The mismatch between state power and state capacity in transnational law enforcement', *Berkeley Journal of International Law,* 22(1): 15–58.

Dalberg. 2013. 'Impact of the Internet in Africa: Establishing Conditions for Success and Catalysing Inclusive Growth in Ghana, Kenya, Nigeria and Senegal', available at: http://www.impactoftheinternet.com/pdf/Dalberg_Impact_of_Internet_Africa_Full_Report_April2013_vENG_Final.pdf (accessed 18.03.2016).

Dusabirane, David. 2015. 'East Africa: Airclerk's CEO envisions a cashless economy in Rwanda', *All Africa,* available at: http://allafrica.com/stories/201511050868.html (accessed 25.02.16).

Fukuyama, Francis. 2014. *Political Order and Political Decay: From the Industrial Revolution to the Globalization of Democracy.* New York: Farrar, Straus and Giroux.

Gady, Franz-Stefan. 2010. 'Africa's cyber WMD', *Foreign Policy,* available at: http://foreignpolicy.com/2010/03/24/africas-cyber-wmd/ (accessed 01.03.16)

Goncharov, Max. 2015. 'Criminal Hideouts for Lease: Bulletproof Hosting Services', Trend Micro report, available at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-criminal-hideouts-for-lease.pdf?_ga=1.24160381.61042644.1458131160 (accessed 18.03.2016)

Gordon, Dorothy and Nii Quaynor. 2015. 'How can the Internet help Africa? Start by asking Africans', *The Globe and Mail,* 5. September, available at http://www.theglobeandmail.com/report-on-business/rob-commentary/how-can-the-internet-help-africa-start-by-asking-africans/article26229308/ (accessed 01.03.16)

Helle-Valle, Jo. 2015. 'What makes a society an internet society?', available at: http://www.mediafrica.no/blog/2015/11/22/is-botswana-an-internet-society (accessed 24.02.16).

ITU. 2012. 'Impact of broadband on the economy', available at: https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf (accessed 23.02.16)

Karambu, Immacuate. 2011. 'Kenya, many banks at risk from cyber crime', *All Africa,* available at: http://allafrica.com/stories/201111040035.html (accessed 01.03.16).

Klimburg, Alexander and Hugo Zylberberg. 2015. 'Cyber Security Capacity Building: Developing Access', NUPI-Report no. 6, 2015.

Kshetri, Nir. 2010. 'Diffusion and effects of cyber-crime in developing economies', *Third World Quarterly,* 31(7): 1057–1079.

Kshetri, Nir. 2013. *Cybercrime and Cybersecurity in the Global South.* New York: Palgrave Macmillan.

Landau, Susan. 2010. *Surveillance or Security – The Risks Posed by New Wiretapping Technologies.* Cambridge, Massachusetts: MIT Press.

Langø, Hans Inge. 2016. 'Cyber Security Capacity Building: Security and Freedom', NUPI-Report no. 1, 2016.

Mbogo, Marion. 2010. 'The impact of mobile payments on the success and growth of micro-business: the case of M-Pesa in Kenya', *Journal of Language, Technology & Entrepeneurship in Africa*, 2(1): 182–203.

Muller, Lilly Pijnenburg. 2015. 'Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities', NUPI-Report no. 3, 2015.

Palmer, Maija. 2016. 'Rogue states play host to outlaw servers', in Financial Times 16. March, 2016, available at: http://www.ft.com/intl/cms/s/2/c926b4ec-da25-11e5-98fd-06d75973fe09.html#axzz434Bv3Q84 (accessed 18.03.2016).

Pawlak, Patryk. 2014. 'Riding the digital wave – The impact of cyber capacity building on human development', *ISS report,* available at: http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf (accessed 18.03.2016).

de Renzio, Paolo, Lindsay Whitfield and Isaline Bergamaschi. 2008. 'Reforming foreign aid practices: what country ownership is and what donors can do to support it,' Global Economic Governance Programme Briefing Paper, Department of Politics and International Relations, *University of Oxford.

Sullivan, Bob. 2007. 'Who's behind criminal 'bot' networks?', available at: http://www.unl.edu/eskridge/cyberbot3.htm (accessed 01.03.16).

Subrahmanian, V.S., Ovelgone, M., dumitras, T., Prakash, B.A. 2015. 'The Global Cyber-Vulnerability Report', Springer International Publishing.

Tafirenyika, Maimba. 2011. 'Information technology super-charging Rwanda's economy', *Africa Renewal,* available at: http://www.un.org/africarenewal/magazine/april-2011/information-technology-super-charging-rwandas-economy (accessed 25.02.16).

Timberg, Craig. 2014. 'German researchers discover a flaw that could let anyone listen to your cell calls', *Washington Post*, available at: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/ (accessed 18.03.2016).

UN. 2015. 'United Nations General Assembly's Overall Review of the Implementation of WSIS Outcomes', available at: http://www.un.org/pga/70/wp-content/uploads/sites/10/2015/08/2015_October_09_World-Summit-on-Information-Society.pdf (accessed 18.03.2016).

Wagley, Rachel. 2014. 'Telecom investments threaten privacy rights in Burma', *US Campaign for Burma,* available at: https://uscampaignforburma.wordpress.com/2014/02/04/telecom-investments-threaten-privacy-rights-in-burma-2/ (accessed 01.03.16).

Were, Daudi Khamadi. 2013. 'How Kenya turned to social media after mall attack', *CNN,* available at: http://edition.cnn.com/2013/09/25/opinion/kenya-social-media-attack/ (accessed 25.02.16).

World Bank. 2016. *World Development Report 2016 - Digital Dividends* Washington DC: World Bank Group

WSIS. 2015.*Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of WSIS Outcomes*, available at: http://workspace.unpan.org/sites/Internet/Documents/UNPAN95707.pdf (accessed 29.02. 16)

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

The project has previously published: 'Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities', by Lilly Pijnenburg Muller, 'Cyber Security Capacity Building: Developing Access' by Alexander Klimburg and Hugo Zylberberg, and 'Cyber Security Capacity Building: Security and Freedom' by Hans-Inge Langø. All available at www.nupi.no

Norwegian Institute of International Affairs

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

About the Author

Dr Niels Nagelhus Schia Nagelhus Schia (@nielsschia) is a senior research fellow at NUPI, he is a former fellow of the NSSR (New School for Social Research), a former Fulbright scholar and head of the scientific committee for the annual Fulbright award in Norway. He holds a PhD degree in social anthropology from the University of Oslo.

Schia's current research focuses on cyber politics, power in cyber space and cyber security, cyber capacity building, and collaboration between states and non-state actors. Schia is head of NUPI's research programme on cyber security, he is project manager for NUPI's current research project on cyber security capacity building, and has previous experience as project leader from several other research projects at NUPI. Schia has published his research in scientific peer-reviewed journals and books. In his capacity as researcher, he has acted as an adviser to governments and international organizations on issues pertaining to cyber security capacity building, statebuilding, peacebuilding and global governance.

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