NUPI Norwegian Institute of International Affairs

Policy Brief
[9/ 2016]

Cyber Security as Development Assistance – Growth and Vulnerability

Niels Nagelhus Schia and Siri Strand

Recommendations

- Digital development needs to be followed up by a focus on digital security. Here donor countries can assist 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.
- Combining development assistance with multilateral diplomacy, through cyber security capacity building (CCB), could provide excellent opportunities for donor countries to strengthen 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 primarily commercial interests have driven digitalization, 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 could help to facilitate this through capacity building and by improving knowledge and expertise in developing countries about CERTs.
- While maintaining the focus and often prioritized collaboration with international organizations such as the UN, EU, NATO and AU, donor countries should also seek ways of working together with major private enterprises, perhaps especially when engaging in development and cyber security.
- 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 donor countries' expertise could be exported, to help in counteracting the hollow digitization of developing countries.
- Other potential niche capabilities for export through development activities include awareness campagnes such as national security month and Security Divas – the latter in particular would readily fit with many donor countries traditions of enhancing and strengthening women's rights and security in developing countries.

Introduction

Connection to digital networks have a fundamental impact on societies, changing not only how individuals and businesses navigate, operate and seek opportunities, but also how governments must act in order to provide efficient and sustainable development assistance. Much policy literature on digitalization and development has focused on the importance of connecting developing countries to digital networks, and how digital networks can expand the access to information for billions of people – and by this, also stimulate economic activity. While there is a wide agreement about the need to bridge the gap between the people who are connected to the digital networks, and those who are not connected, a topic that is often neglected is the new societal vulnerabilities emerging from digitalization in developing countries.

The importance of digital technology underpins most of the social, economic and political development goals of most donor countries and international organisations 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.[1]

In the NUPI project 'Cyber Security Capacity Building (2015-2016) we have mapped out concrete risks and challenges, proposed recommendations for dealing with them, and provided suggestions for implementing the adequate tools effectively. This policy brief presents a summary of the final report, which draws on project reports produced by NUPI related to this project.[2]

Digital Dividends in Developing Countries

New Information- and communication technologies (ICT) are contributing to growth and development in developing countries through increased productivity, by providing public and

[1] 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).

[2] Schia 2016.

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 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).

Donor countries and international organisations seize on digitalisation as an opportunity to fight poverty. However, digitalization in countries that suffer from lack of development, poor governance and poverty might 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 development goals and intentions in donor policies, and digital vulnerability and cyber security in developing countries.[3] In order to be sustainable, digital development must be followed up by a focus on digital security.

Weak technological environment

Digital technology has been used in Africa to strengthen internal solidarity and economic growth. In 2007, the telecom company Safaricom 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. 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 donors following the attack (Were: 2013). A few years earlier such mobilization would not have been possible. Carl Bildt, former prime minister and foreign minister of Sweden, is among those who have argued that information technology (IT) has the potential to become the most important tool for development to billions of people living in Africa and Asia (Bildt 2015).

While the benefits from internet connection and digitalization are evident, there are still many hurdles that has to be dealt with before most people in developing countries can enjoy extensive use of the Internet. 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.[4]

The need to build an accurate environment for technology before business can begin to thrive and then reap the benefits of digital connectivity has been emphasized by international organizations and policy-makers (see for instance ITU 2012, WDR 2016). Further research has pointed out the similar direction, like the Dalberg Report (2013) which 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 a well-functioning internet economy is thus dependent of a set of conditions for usage, such as costs, education and relevance of services. These conditions are in turn influenced by the degree of access, relevance, availability and attractiveness. Core traditional development politics and projects might, therefore, become central elements for bridging the digital divide.

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.

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. However, user conditions and Internet accessibility/availability are very much conditioned by the middle mile, the national backbone and inter-city 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 marked 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 'super-served', while the rest of the country is underserved (WDR 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. Whereas the developed countries 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 (WDR 2016: 208). Development efforts needs to focus on bridging this infrastructural gap, as a key determinant in an enabling business environment (Klimburg and Zylberberg 2015: 9).

[3] 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.

[4] See Schia 2015.

Developing countries and new kinds of societal vulnerabilities

ICT has become a highly important foundation for most infrastructures in developed societies, and individuals, businesses, and nations are depending more and more on data and systems in the virtual world. Although developing countries are now following the path of developed countries and become 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, came the addition of mobile phones, the Internet, and smartphones. Developing countries, by contrast, are leapfrogging straight into wireless technology and mobile devices, and Internet networks are often built by the private sector. This means that digital technologies are being put to use before functional, regulatory mechanisms have been developed and put in place. This opens 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 focusing on awareness, knowledge, information, education and employment. In this context, Cyber Security Capacity Building (CCB) becomes integral to development.[5]

The Security-Development nexus

Drawing on the scholarly tradition on the security-development nexus, Klimburg and Zylberberg (2015) identify Cyber Security Capacity Building (CCB) as a key component of development. They hold that this combination is particularly important because: "... the areas with the highest potential for economic growth correspond roughly with those where the security risks are the highest [and] the skills developed locally through cyber security training 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).

The NUPI project 'Cyber Security Capacity Building' (2015-2016) 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 hosts 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).

International cyber politics and developing countries as potential swing-states

Due to 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 new political landscape, there is a dire need for new norms, policies and trust-building measures.

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. While international bodies like the UN, EU and NATO are important players in developing international cyberspace policy, the technical revolution is run by the private sector. Thus, while maintain its focus and prioritize collaboration with international organizations, 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 discussions about cyber politics in the global arena. Through development assistance, focusing on cyber security capacity building (CCB), there is a potential for developing cooperation and partnerships with developing countries, in our effort towards a secure and sustainable cyberspace. As pointed out in a recent NUPI Report, the dichotomous character of 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 organizations, and decision makers from donor and recipient countries seems the most natural way to explore these links and identify potential partnerships for cyber policy in international forums. Thus, CCB seems set to become an increasingly important arena for international diplomacy.

Norway has the comparative advantage of a long tracked 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 the UN Sustainable Development Goals (SDG) commitments by contributing to the digital revolution in developing countries.

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 the cyber security capacity building (CCB) projects. Because of the role assumed by the private sector in the digital revolution, the public-private relationship in this field should also be viewed in terms of 'ownership'.

[5] See also Pawlak 2014.

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. 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 that has previously been 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.

Conclusion

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 experiences from traditional donor countries to the developing countries become 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.

The Cyber Security Capacity Building project (2015-2016) 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.

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 emphasised. Building capacity in cyber security represents a relatively new political field, not properly included in the UN's Sustainable Development Goals (SDG) 2015, and neither in the World Bank's World Development Report – Digital Dividends (2016). 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 a free flow of information – trigger new kinds of challenges with regard to international politics and diplomacy. Managing such challenges will require an in-depth understanding of the democratic, social and economic development contexts on which cyberspace depends.

NUPI Norwegian Institute of International Affairs

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

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

About the authors

Niels Nagelhus Schia 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 and cyber space, cyber security, cyber capacity building and collaboration between states and non-state actors. Schia is head of NUPI's research programme on cyber security and project manager for NUPI's current research project on cyber security capacity building.

Siri Strand is a research assistant in the Research group on Security and Defence at NUPI. She holds an B.A. in International Studies from the University of Oslo and has also studied in Washington DC. Strand's research interests include cyber security capacity building, development, cyber warfare and Internet governance.