Routledge
Taylor & Francis Group

Third World Quarterly

ISSN: 0143-6597 (Print) 1360-2241 (Online) Journal homepage: http://www.tandfonline.com/loi/ctwq20

The cyber frontier and digital pitfalls in the Global South

Niels Nagelhus Schia

To cite this article: Niels Nagelhus Schia (2017): The cyber frontier and digital pitfalls in the Global South, Third World Quarterly, DOI: 10.1080/01436597.2017.1408403

To link to this article: https://doi.org/10.1080/01436597.2017.1408403

Published online: 11 Dec 2017.

THIRD WORLD QUARTERLY, 2017
https://doi.org/10.1080/01436597.2017.1408403

The cyber frontier and digital pitfalls in the Global South

Niels Nagelhus Schia

Centre for Cyber Security Studies, Norwegian Institute of International Affairs (NUPI), Oslo, Norway

ABSTRACT

How does digitalisation lead to new kinds of global connections and disconnections in the Global South? And what are the pitfalls that accompany this development? Much of the policy literature on digitalisation and development has focused on the importance of connecting developing countries to digital networks. 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. However, the rapid pace of this development implies that digital technologies are being put to use before good, functional regulatory mechanisms have been developed and installed. The resultant shortcomings – in state mechanisms, institutions, coordination mechanisms, private mechanisms, general awareness, public knowledge and skills – open the door to new kinds of vulnerabilities. Herein lie dangers, but also opportunities for donor/recipient country exchange. Instead of adding to the already substantial literature on the potential dividends, this article examines a less studied issue: the new societal vulnerabilities emerging from digitalisation 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.

ARTICLE HISTORY
Received 3 March 2017
Accepted 20 November 2017

KEYWORDS
Digitalisation
Sustainable Development Goals
digital dividends
cybersecurity
cybersecurity capacity building

Introduction

The leap into the digital age has reached the Global South, providing more and more people with digital technology, new opportunities, and greater connectedness. But the rapid digitalisation of the Global South has also opened the way to new kinds of vulnerabilities within these countries. The introduction of this technology has often outpaced the establishment of state institutions, legal regulations and other mechanisms that could help to manage the new challenges that arise.

This article examines the little-studied issue of the new societal vulnerabilities emerging from digitalisation in the Global South. There is broad agreement about the need to bridge the gap between the connected and the disconnected, but the pitfalls are many, especially concerning cybersecurity[1] – a topic often neglected, also in the World Bank report *World*

CONTACT Niels Nagelhus Schia nns@nupi.no

Development Report 2016 – Digital Dividends.[2] Here I attempt to redress these shortcomings, using an analysis of the cyber frontier to highlight cultural (trans)formation and continuity.[3] By the 'cyber frontier' I mean the interface regarding digitalisation, between local and national polities in the Global South and large-scale global forces. This perspective highlights digitalisation as a process in which polities and communities are produced locally, and become (trans)formed through their entanglement with external digital connections.

The cyber-frontier perspective makes clear how the Global South's participation in digitalisation is not simply a matter of *joining cyberspace*: it is a question of selective forms of global connection in combination with disconnection and exclusion. Firstly, I contextualise security concerns and digital pitfalls, describing the trajectory of digitalisation in the Global South and how it diverges from that of the more industrialised countries. Selected empirical snapshots show the current situation in several countries of the Global South. I then explore how 'technological leapfrogging' is interlinked with the risk of greater societal 'hollowness',[4] where new and unprecedented societal vulnerabilities may emerge. 'Hollowness', in this context, results from the lag between technology development on the one hand and societal capacity and management of this technology on the other. This hollowness refers to weak or inadequate institutions, policies and strategies, poor organisational and individual defence mechanisms, lack of standards, greater recruitment to cybercrime due to high unemployment and low wages, and a lack of capacity and legal frameworks to manage risks and vulnerabilities in the society.[5] The various ways of managing this hollowness at the cyber frontier affect nations and individual citizens, but also the global stability of cyberspace. The digital pitfalls cause societal vulnerabilities that can be addressed by linking digitalisation with security and economic growth through a focus on building cybersecurity capacity.

Focusing on cybersecurity in connection with development assistance and implementation of the United Nations (UN) Sustainable Development Goals (SDGs), I argue that an overly unilateral focus on connectivity for combating poverty may end up propelling hollowness and digital pitfalls rather than sustainable growth. Finally, I explain how this triple knot, digitalisation, security and economic growth, represents an opportunity for renewed collaboration between donor and recipient countries that can build on local and national contexts and continued engagement in the Global South.

Digitalisation of the Global South and the SDGs

Digital technology underpins most of the social, economic and political development goals of donor countries and international organisations today. Promoting, cultivating and encouraging growth and stability in recipient countries through digitalisation, and capacity building in cybersecurity, will play an important role in future foreign policy considerations and government programmes.[6]

There are two main reasons why building cybersecurity capacity will be increasingly important with regard to the cyber frontier and the Global South: (1) Access to cyberspace is essential to social, economic and political stability. If digital systems are adopted without being secured, high levels of Internet penetration might instead contribute to destabilising governments, national election systems, media environments and public discourse, disrupting political and democratic stability. Securing new digital systems is thus essential. (2) The countries of the Global South are increasingly hosting the infrastructure and actors behind malicious cyber activities. This makes capacity-building measures important both for enhancing national security, and for responding to cyberthreats in donor countries.

Although information and communications technology (ICT) has been around for almost half a century, digitalisation and cyberspace represent a fairly new field in international politics (global economic, security and human rights agendas), and an even more recent addition to the field of development assistance. In 1999, the first UN resolution addressing cybersecurity was adopted, marking the starting point for multilateral, intergovernmental efforts to deal with cybersecurity. The first UN resolution pertaining to digitalisation and development assistance came in 2001, when the General Assembly decided that a World Summit on the Information Society (WSIS) should be held. The inaugural meeting was held in Geneva in 2003, and the second in Tunis in 2005; these were followed up by a WSIS+10 in New York in 2015. Because the goal of the first summit was to provide a foundation for an information society for all, this meeting had implications for development politics as well.[7] In 2004, the Partnership on Measuring ICT for Development was launched as a multi-stakeholder initiative to improve the situation in the Global South. In 2005, the second WSIS meeting emphasised implementation and financing mechanisms, as well as Internet governance.[8] Multiple stakeholders broadly supported the outcome resolution of the Geneva and the Tunis meetings. Since then, the pace of policymaking has increased rapidly. New paths for policymaking have emerged, especially regarding cybersecurity, cybercrime and Internet governance. Now the cyber and development highway also seems to be gaining momentum. In 2015, the WSIS+10 high-level meetings issued recommendations on how to proceed in further connecting countries in the Global South, and called on all 'governments, the private sector, civil society, international organisations, the technical and academic communities and all other relevant stakeholders to integrate information and communication technologies in their implementation approaches to the SDGs'.[9]

Since 2000, the cyber frontier has gained new terrain. There has been a considerable increase in connectivity, creating new tools for economic growth and social development – and there is no reason to believe that this trend will not continue.[10] Connections have been made between the WSIS+10 and the SDGs, such as action lines for achieving these goals through digitalisation.[11] These initiatives have drawn considerable international attention to this agenda, with digitalisation increasingly recognised as a precondition for sustainable development.[12]

However, the potential pitfalls are many. Digitalisation in countries that suffer from lack of development, poor governance and poverty may provide new breeding grounds for cybercrime. Baseline studies have demonstrated the gap between the development goals and intentions in donor policies, and digital vulnerability and cybersecurity in developing countries.[13] To be sustainable, digital development must be concerned with digital security. This, in turn, will require core development assistance focused on improving and securing the digital systems as well as the analogue foundations for digital technology, including governance, knowledge, information, education, employment and appropriate institutions.

The cyber frontier and new societal vulnerabilities

Individuals, businesses and nations are depending more and more on data and digital systems. The Global South is following suit, rapidly expanding the cyber frontier. 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 like

energy, power, economy, health, communications and transport. The increasing interconnectedness of these features entails a major change in societal risk factors, highlighting the close linkages between the domestic and international dimensions of politics. Global, complex and rapidly shifting trends impinge on domestic political contexts, especially as regards the security dimension. Along with the opportunities and possibilities shaped by the digital revolution come new and more transnational challenges to major areas of societal infrastructure as well as industry, innovation and business. These threats cannot be reduced to technological concerns: they are intertwined with international politics and global trends. Countries in the Global South with poor infrastructure and governance are rapidly gaining connection to the Internet – but the digitalisation of these countries is often hollow. This can provide opportunities for ill-intentioned cyberspace actors whose activities may affect not only domestic problems in these countries, but global society as well. Cybercriminals gravitate towards the points of least resistance – jurisdictions with little cybercrime legislation and weak law enforcement – to conduct attacks on the networks of other countries. This makes cybersecurity capacity a regional and transnational issue, and one where countries with more sophisticated capacities can assist 'weak link' countries.

Although the nations of the Global South are following in the path of the Global North and becoming more aware of cybersecurity needs, they are taking a different route. For the Global North, digitalisation 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 the infrastructure gradually established over more than a hundred years, came the addition of mobile phones, smartphones and the Internet. By contrast, the countries of the Global South are leapfrogging straight into wireless technology, with mobile and Internet networks often built by the private sector (obviating the need for investments in expensive copper-cable wiring). Jumping headlong into the digital age has indeed provided impoverished countries in the Global South with digital technology, new opportunities and greater connectedness. But the introduction of technology has often outpaced the establishment of state institutions, legal regulations, and other mechanisms that could manage the new challenges arising from this technology. Digital technologies are being put into use before adequate functional and regulatory mechanisms have been developed and installed. The resultant shortcomings – in state mechanisms, institutions, coordination mechanisms, private mechanisms, general awareness, public knowledge and skills – produce hollowness and open the way to new kinds of vulnerabilities.

Countries in the Global South are weak in the know-how, awareness, institutions and skills needed for dealing with cybersecurity issues. This weakness constitutes a challenge with many similarities to prior transitions and revolutions in economic life. Including the perspectives of local and national stakeholders at the cyber frontier can ease potential fallacies similar to those from the first and second waves of imperialism, helping to counteract tendencies that could drive 'digitalisation' towards a third wave. Here we see historical continuity to 'the global digitalisation project'. The continuity is represented by how the three waves caused challenges pertaining to new technology and regulation also in the industrialised world. Indeed, these challenges are not unique to the Global South: Organisation for Economic Co-operation and Development (OECD) economies also face problems in regulating technology that has already been deployed. But the societal vulnerabilities and digital pitfalls distinct to the Global South appear more acute, hollowing out the sustainability ambitions expressed in the SDGs and the ambition to combat poverty through digital connectivity.

This vulnerability can be tackled through development assistance to projects and activities focusing on awareness, knowledge, information, education and employment. Here, digitalisation and building cybersecurity capacity become integral to development assistance and the SDGs – and can help to make countries in the Global South more competent actors in the global arena where international cybercrime is being fought.

The security/development nexus

Combining cybersecurity with development assistance may be contentious, giving rise to concerns about the securitisation of development assistance from the development community. Conversely, linking cybersecurity with development assistance may contribute to de-securitising it. In any case, policymakers are increasingly recognising cybersecurity capacity as a key component of development assistance. 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 cybersecurity trainings correspond to those needed to enable local businesses to scale up, without having to rely on outside, more expensive talent.[14]

Models for building cybersecurity capacity generally operate with three categories: technological, human and organisational resources. Although helping to provide access to information and communication technology is recognised as an important part of the development agenda,[15] it is the building of institutional and human resources that should be the main priority of donor-country development policies.

In the Global South, Botswana, Kenya, Mozambique, Myanmar, Rwanda and Tanzania have been experiencing rapid growth in digitalisation and digital connectivity. This connectivity fuels social, cultural, political and economic (trans)formation, changing people's everyday lives. The upside of this digital revolution is that it can help people out of poverty, turning the economies in certain countries of the Global South into some of the fastest growing in the world. When local 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 and fishermen, as well as small and medium-sized businesses, can put to good use. However, there are also disadvantages. The digital trajectories of countries in the Global South often involve a different set of cyberthreats than those experienced elsewhere. Bot herders[16] and other cybercriminals tend to come from locations where high-paying ICT jobs are rare or unavailable;[17] throughout the Global South, the growth of IT jobs is generally lower than the growth of Internet penetration.[18]

The lack of capacity can stem from technological, behavioural and policy-related factors. Generating innovation driven primarily by commercial forces, without attention to security, has left digital hollowness in these countries. It has become easy to target unprotected devices and unskilled users, making these countries attractive to cybercriminals. Many countries in the Global South also lack the resources to build institutions to combat transnational crime.[19] Laws that recognise cybercrime, law enforcement mechanisms and personnel who understand cybercrime, as well as the awareness necessary for dealing with cybercrime – all these remain inadequate. With weak institutions, limited capacity and generally low resources

for fighting cybercrime, these countries are likely to remain attractive for cybercriminals also in the future.

Unless sufficient attention can be paid to analogue foundations, this hollowness may escalate when countries in the Global South invest in more sophisticated ICT technology and digital connectivity. In addition to investments in security measures, such as anti-virus programmes, it is essential to improve basic knowledge about ICT. For instance, both the public and private sectors in the Global South lack common sets of standards and are more likely to skip new security updates than digital networks in countries with more advanced cybersecurity capacities, and thus more easily become infected with viruses and malware. Additionally, digital infrastructures in the Global South (as in Myanmar) are often based on mobile broadband access and not fixed broadband. Slow speed and poorly updated digital networks mean greater vulnerability to DDOS attacks – like those in Myanmar in 2010, Estonia in 2010 and Georgia in 2008 – and make computers easy targets for bot-net operators.[20] In addition to the software and digital infrastructure challenges, poor and fragile institutions have contributed to this digital hollowness. Rogue states and countries in the Global South become hosts to outlaw servers, so-called 'bulletproof hosting'. The hosts of these servers operate beyond the reach of most law enforcers, and make possible cybercrime elsewhere.[21] Studies have shown how certain vulnerabilities in the global network, such as those in the SS7 (the network that allows cellular carriers to route calls, texts and other services to each other), built in the 1980s, can be used for surveillance by persons with illicit intentions, potentially undermining the privacy of cellular customers.[22] 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'.[23]

Weak institutions and law enforcement mechanisms on cybercrime contribute further to the digital hollowness of countries in the Global South. Digitalisation can be a key factor for economic and social development, and even democratisation – but such development also opens new frontiers for criminals and others with malicious intentions. Digitalisation holds the potential to be either a boon or a threat to democracy. While it can help facilitate peaceful opposition and government rule-of-law enforcement, it can also be used for violent rebellion or repressing the population. Policymakers concerned with building cybersecurity capacity increasingly take such threats and risks into account when engaging in development assistance. A country's analogue foundations will usually determine the direction of its digitalisation.[24]

Cybersecurity plays a key role in ensuring sustainable economic and social development as well as in achieving the international goals of combating poverty and inequality by 2030. Therefore, needs-assessments of cybersecurity maturity in the Global South will become a mapping activity increasingly applied in development assistance.[25] This includes the rule of law, education and programmes to promote small- and medium-sized businesses, as well as donor programmes aimed at facilitating the participation of recipient countries (civil society and governments) in a multi-stakeholder approach to Internet governance.

Digital pitfalls in the Global South

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. Perhaps it will be possible to achieve this, because the Global South is changing fundamentally, thanks to the connectivity made

possible by digital networks. Nevertheless, achieving faster growth, more jobs, better services and broader benefits will be challenging, and can be endangered through cybercrime. In the following, I examine digital pitfalls at the cyber frontier in terms of weak technological environment, national cybersecurity strategies and policies, banking and mobile money, poor network infrastructure, and urban-centred digitalisation.

Weak technological environment

International organisations and policymakers have emphasised the importance of building a suitable environment for technology in order for businesses to begin to thrive and reap the benefits of digital connectivity.[26] Research has pointed in a similar direction, framing cybersecurity capacity building as essential for achieving economic growth, but also for supporting the stability of cyberspace. This will necessitate a pairing of international aid and issues of law enforcement. Drawing on a survey of more than 1300 businesses, 1000 small- and medium-sized enterprises, and extensive interviews in Ghana, Kenya, Nigeria and Senegal, the 2013 Dalberg Report describes the digitalisation of these countries as a work in progress, with potentials still largely untapped. Further, it identifies 'core infrastructure' and 'conditions for usage' as the two key pillars of a well-functioning Internet economy.[27] Core infrastructure requires an environment with affordable mobile and Internet access – but also with electricity, skills, knowledge, education and appropriate legislation. Establishing such an environment hinges on various conditions including costs, education, institutions and relevant services. These conditions are, in turn, influenced by the degree of access, awareness, availability and attractiveness. Thus, digital dividends need to be built on analogue foundations – and that makes traditional core development politics and projects central elements in bridging the digital divide.

To illustrate and contextualise the importance of this aspect, I draw on studies of countries in the Global South currently experiencing rapid digitalisation, in addition to my own fieldwork in Myanmar in 2016, and international cybersecurity diplomacy.

Lack of national cybersecurity strategies

Since not all cyber incidents can be prevented, and greater digitalisation and connectivity will increase the potential for cybercrime incidents, countries will also increasingly need to cope with such problems. But with the fast pace of the digitalisation in many countries in the Global South, many are lagging behind when it comes to developing plans and strategies on how to resist, recover and respond to cyber incidents. Protecting a nation's critical infrastructure and cybersecurity requires comprehensive national strategies that include setting priorities, determination of areas of responsibilities, the responsibilities and mandates of key actors, and allocation of resources. National cybersecurity strategies are necessary in order to improve cyber resilience and to improve the capability for tackling cyber incidents, whether it is in order to protect against cybercrime or cyberattacks. Furthermore, a state's responsibilities vis-à-vis other states will require capacities to respond to cyber incidents. The UN's Group of Government Experts (GGE) has taken steps towards emplacing responsibilities under international law on states to assist and respond to request from other states whose critical infrastructure has been attacked or subjected to malicious attacks.[28] Scholars such as Mark Raymond have stressed the need to enhance the capability of managing such challenges by

cultivating responsibility regarding troubleshooting.[29] Cybersecurity capacity building becomes integral to the fulfilling of states' international responsibilities and obligations.

Today, many countries of the Global South – among them Bhutan, Myanmar, Tanzania and Uganda – have no published, officially recognised national cybersecurity strategies, or designated overarching units or institutions to coordinate national cybersecurity. Additionally, many countries, including those just mentioned, lack institutions to oversee and protect their digital critical infrastructure and thus also formal collaboration between the government and owners of critical assets. In Myanmar, a country currently experiencing perhaps the world's most rapid increase in Internet users, digitalisation has outpaced attention to many security aspects: 'the government is concerned with e-government and e-commerce. Cybersecurity is not their priority right now. The Government's focus is on becoming digital. The lack of personnel and policy makes it difficult to incorporate an overarching and coordinated focus'.[30] Weaknesses in national political framework capabilities and available resources impact on the resilience of countries in the Global South towards cybercrime and cyberattacks, but also concerning the emerging global responsibility to troubleshoot.

Digitalisation and economy

In Africa, digital technology has also been used 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 north-east of the country (as with the 2011 Kenyans for Kenya campaign). In 2007, the telecom company Safricom launched the mobile money service M-PESA: it attracted six million customers within two years, transferring billions annually. M-PESA was launched in Tanzania in 2008,[31] and has since expanded to Afghanistan, Albania, Egypt, India, Lesotho, Mozambique, Romania and South Africa. Through M-PESA, persons without bank accounts can leapfrog from traditional finance arrangements and into the digital economy.[32] Another African country that has caught the digital wave is Rwanda. Considerable investments have been made in digital 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'.[33] 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. This initiative was part of the government's Smart Kigali programme for rapid modernisation and digitalisation of the nation's capital.[34]

Similar things are happening with many countries in Asia. Myanmar, for instance, is experiencing perhaps the fastest rollout of telecom infrastructure in history. While broadband penetration remains low, the mobile market has grown rapidly since 2013 when the telephone operators Telenor and Ooredoo entered the market, and is expected to reach 97% of the population of Myanmar by 2021.[35] Mobile money represents a major opportunity for a country where only 20% of the population have bank accounts. Mobile operators are seizing this opportunity and tapping into the mobile money market. Three of the country's biggest mobile operators are currently teaming up with Myanmar banks to launch new mobile money services. Telenor launched its Wave Money service in October 2016; the company intends this to be available in all states and regions of Myanmar and had more than 10,000 wave shops across the country by the end of 2017.

With the rapid development of digital payment systems come new employment opportunities, economic growth and means of exchange. However, the sheer pace of this expansion also provides potential openings for cybercriminals. In some countries of the Global South, banks lack resources and the human capacities to invest in cybersecurity. With the lack of resources and the fact that cybersecurity standards often are the responsibility of the company and not a regulatory body, banks might opt to cover the costs of security breaches rather than invest in implementing cybersecurity standards – so even banks may contribute to producing 'hollowness' and antitrust. The robberies of the Bangladesh National Bank in 2016, Banco del Austro in Ecuador in 2016, and in the Philippines and Vietnam in 2015, are important reminders that cybercriminals may move towards less developed regions as digital connectivity and opportunities emerge and progress. This is increasingly becoming a pressing issue in the Global South, where security measures are weaker than those in financial hubs like London and New York.

Moreover, through international financial systems like Swift, these hubs are interconnected with other banks around the world. Thus, even banks that have their own security measures in place may become compromised through smaller banks, for instance in the Global South, which have not been able to step up their security protocols. Cyberattacks on banks in the Global South could damage not only the economy of the banks in question and their customers, but also global finance, because larger banks could become reluctant to transact with smaller banks in the Global South.

In many cases, there is a dire lack of national policy, regulations, insurance and customer protection.[36] Efforts are often made within rather than across sectors, with the private sector and telecommunication sector taking the lead, often in an ad hoc manner. Establishing a broader set of policies and regulations requires a fine-tuned collaboration between regulator and provider. One way of dealing with this challenge could be for governments or a regulatory body to identify incentives and specify cybersecurity standards for all sectors.

The adoption of blockchain could also mitigate some of these vulnerabilities, but the economies of the Global South will encounter various challenges before this can be used. Among the major challenges and obstacles are the additional bandwidths required. This is likely to be a severe problem in the Global South, already facing network congestion and institutional bottlenecks that will hamper the implementation of new technology.[37]

While the digital dividends in the Global South are evident, there are still many hurdles to be dealt with before the general populace can enjoy extensive use of the Internet. 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:[38]

> 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% of her monthly income on phone calls and texting. And many poor lack the basic literacy and numeracy skills needed to use the internet.[39]

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 helping to improve the technological business environment in the Global South.[40]

Poor network and infrastructure: urban-centred digitalisation

The World Bank has developed a tool for measuring the degree of connectivity. To measure the availability, accessibility and affordability of digital networks and infrastructure, this infrastructure is divided into 'three miles': the first mile is the level where the Internet enters a country, the middle mile is where the Internet spreads through the country, and the last mile is where the Internet actually reaches the end users. Additionally, an 'invisible mile', involving important but less visible elements necessary for maintaining the integrity of these three levels, is often included in this division of infrastructure.[41] This tool is also useful for capturing pitfalls and vulnerabilities pertaining to the cyber frontier. Much has been done in African countries 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 (eg SEACOM) and West Africa (eg WACS) have been bringing faster Internet to the continent, providing countries such as Djibouti, Ghana, Ivory Coast, Kenya, Madagascar, Mozambique, Nigeria, Senegal, South Africa, Sudan and Tanzania with high-speed services.

In Myanmar, however, the infrastructure is disproportionately based on mobile broadband access, not fixed broadband.[42] The World Bank has highlighted this as problematic in several developing countries, as wireless alternatives are not a full substitute for fixed-line networks, often being more expensive and slower. This creates a subdivision of Internet coverage into different leagues, with developing countries stuck with a lower quality coverage.[43] Slower speeds also mean greater vulnerability to DDOS and other attacks, as occurred in Myanmar during the run-up to the 2010 general elections.

While Myanmar is experiencing a more rapid pace of digitalisation than most other countries, it is nevertheless a typical case of early-stage Internet development. But the pace of digitalisation makes the challenges very distinct and visible, so the country offers good opportunities to identify, study and learn how to mitigate digital pitfalls. While there has been immense growth in Internet coverage nationally, through the building of mobile towers and mobile Internet, the underlying structure and backbone of the Internet remains weak. This is important, as most websites, both foreign and domestic, are based on servers outside the borders of Myanmar. Stable connections to the outside world are essential for gaining access to the most frequently used websites.

The government controls the sole Internet Exchange Point (IX) in the country. Thus, all data traffic in and out of Myanmar is in government hands, entailing privacy risks and the threat of data infiltration.[44] Until recently, Myanmar was served by a single submarine cable, a glaring vulnerability in any country's cybersecurity setup[45] – as demonstrated by the 2010 DDOS attack and an accidental severing of the cable in 2007, both instances that left the country without Internet coverage for some time. In late 2016 and early 2017 came two new connections to the submarine cable network – through the SEA-ME-WE-5 consortium and the Asia Africa Europe (AAE1) connection. However, these new connections will remain under government control, making the foundations for a secure and open Internet infrastructure limited at best (Calderaro 2016).

Governments can negotiate higher Internet speed, better prices and greater bandwidth – but user conditions and Internet accessibility/availability also depend on 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 market competition

vary from one country to another, affecting the user side of digital networks and infrastructure. Liberalising the market for the middle mile is an effective way of providing open access and the Internet to end users – but, as the World Bank has pointed out, this entails the risk 'that the most popular routes – say, between the two main cities – are 'superserved' while the rest of the country is underserved'.[46]

In the Global South, the last mile is rarely served through fixed copper cables, as local access to networks is dominated by wireless alternatives. This is where the digitalisation trajectory of the Global South differs most from that of the Global North, due largely to the differences between fixed and wireless networks. Whereas the Global North had achieved almost universal fixed-line access before wireless technology took over (ca 2001), most countries in the Global South have never built fixed-line networks. The World Bank report 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.[47]

The 2016 World Bank report goes on to describe how countries in the Global South will have to struggle to achieve a fully sufficient middle mile, or a national backbone. Some countries may achieve this through private–public partnerships, but creating fixed-line networks in rural areas remains challenging and not very likely. Moreover, fragile states, such as the Democratic Republic of Congo and South Sudan, are unlikely to get fixed-line access, even in urban areas. As Klimburg and Zylberberg point out, Internet availability and adequate backbone network infrastructure, network ownership and the geographic patterns of network development are essential for better business environments and improved digital dividends.[48] Furthermore, they hold 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'.[49] The World Bank report finds that the final mile is totally lacking in many countries – including Botswana, Burkina Faso, the Central African Republic, DR Congo, Gabon, Kenya, Rwanda, Swaziland, Tanzania and Togo.[50] In these countries, the analogue foundations for digital enterprises are weak, with no incentives for digital companies, such as online retailers. Unless global donor initiatives intervene, this situation is likely to lead to urban-centred digitalisation in the Global South, with new kinds of societal vulnerabilities and a widening gap between the connected and the disconnected.

Some of the problems obstructing development, such as bad infrastructure and the need for regulation reform, will not vanish as a result of digitalisation – they might even get worse. This underlines the importance of a wider set of issues, including cybersecurity, as an integral element of the development agenda, as the creation of secure networks is crucial for being able to harvest the benefits.

Recent developments have highlighted the vulnerabilities of developing countries, particularly the spread of the 'WannaCry' ransomware in May 2017. This ransomware was spread to more than 100 countries by exploiting a vulnerability in the Microsoft operating system that had been patched some months earlier. However, the updates and patches that protected against the malware were phased out for older versions, or not provided at all for pirate versions. The result was an extensive spread of the ransomware. In Hospitals in the UK were hit, the interior ministry in Russia, telecoms in Spain, the police in India and transport

in Germany. Borders are irrelevant and countries cannot safeguard its people in isolation. Countries which relied heavily on pirated operating systems were particularly hit.[51] Older versions of operating systems are generally more common in countries that have less of the required capital needed to upgrade them. For instance, Windows 7 – the operating system most vulnerable to the WannaCry attack – enjoys a 55% market share in Africa, where it is the most popular operating system by far. By contrast it has a market share of around 40% in Europe and is trending downwards, recently overtaken by Windows 10.[52] This points towards a scenario where developing countries get stuck with ageing and increasingly outdated software, entailing further security risks.

Conclusions

This article has drawn on the cyber-frontier perspective in order to highlight pitfalls pertaining to security and development assistance. New kinds of societal vulnerabilities are emerging, and new power relations are being forged. By emphasising (trans)formation and continuity, my analysis has shed light on the connections between digitalisation, economic growth and cybersecurity. This triple knot indicates a development where the 'haves' can reap digital dividends, leaving the 'have-nots' behind. The growing digitalisation of the Global South also entails a need for greater development assistance and engagement. Further, bridging the digital divide requires analogue foundations, knowledge, awareness and a digital environment in which the focus on cybersecurity will be increasingly important.

There are opportunities for renewed collaboration between recipient and donor countries here. Digitalisation brings with it a pressing need for knowledge, education, institution-building and experience-sharing among countries and regions. Traditional development mechanisms can be applied to enhance sustainable development and cybersecurity capacity, but new aspects and dilemmas are also emerging. The trajectory of digitalisation in the Global South has produced a situation where private actors have assumed a dominant role. Greater collaboration between public and private actors is essential. Distinct local and national patterns apply in countries in the Global South, but also donor countries are struggling with public–private collaboration on cybersecurity, so exchange of experiences can be useful. For donors, this represents an opportunity as well as a challenge, because many of the structural assumptions about ownership, authority and governance that have underpinned traditional development policies are now turned upside down. The few attempts at studying and better understanding these challenges – for instance under the Global Forum on Cyber Expertise,[53] WSIS and the University of Oxford's Global Cyber Security Capacity Centre (GCSCC) – are more broadly focused on policymaking and global challenges, with scattered efforts at understanding the distinct challenges to the Global South and the cyber frontier.

Clearly, there is a potential for more focused and systematic scholarly research and data collection that could underpin donor countries and help to facilitate programmes and processes for dealing with the challenges of the cyber frontier. Building cybersecurity capacity in existing local polities and communities and understanding how these become (trans) formed through their entanglement with global digital connections, international policies and regulations is more important than ever. This calls not only for more research and data collection, but also for better inclusion of developing countries in global arenas where international norms and global governance on cyberspace are being produced.

The distinct properties of cyberspace – it has no borders, has few rules, and involves the free flow of information – trigger new kinds of challenges with regard to international politics, security politics, sustainable development and implementation of the SDGs. This examination of the cyber frontier has highlighted the technological, organisational and human dimensions as well as the local, national, regional and international levels of digitalisation. Building capacity in cybersecurity represents a relatively new political field not properly included in the UN's SDGs or even in the World Bank's 2016 *World Development Report*. The cyber-frontier perspective employed in this article has indicated several potential pitfalls. These challenges will require deeper understanding of the national and local analogue foundations on which the cyber frontier depends.

Disclosure statement

No potential conflict of interest was reported by the author.

Acknowledgements

I am grateful to colleagues how have provided input to an early version of this text and to TWQ's peer reviewers for good comments and suggestions. I am also grateful to the Norwegian MfA who contributed with funding to the research project *Cyber Security Capacity Building - Bridging the digital divide and strengthening sustainable development.*

Note on Contributor

Niels Nagelhus Schia is a senior research fellow at NUPI and holds a PhD in social anthropology from the University of Oslo. Schia is head of NUPI's Cyber Security Centre and his research focuses on the role of cybersecurity in international relations. He conducts academic studies and provides expert analysis and strategic policy advice with regard to cybersecurity. Current studies are concerned with state-behaviour norms, development assistance, societal vulnerabilities, and sovereignty in cyberspace. Schia has also worked on international organisations and statebuilding over the previous years. He has acted as an adviser to governments and international organisations on issues pertaining to capacity building, institution building and global governance. He has participated in international discussions and working groups in the United Nations and regularly participates at international conferences. He is a former Fulbright scholar and head of the scientific committee for the annual Fulbright award.

Notes

1. Cybersecurity is closely interlinked with the security of cyberspace. The linkage between cybersecurity and national security is well established and uncontested. Cybersecurity in the technical sphere refers to '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'(Cavelty, "Cyber-Security and Private Actors," 89). In national settings, it refers to 'the security one enjoys in and from cyberspace' (ibid., 91).
2. World Bank, *World Development Report 2016*.
3. The term 'cyber frontier' is inspired by Igor Kopytoff's 1987 analysis, *The African Frontier*.
4. Kshetri, *Cybercrime and Cybersecurity in the Global South*, 153.

5. Kshetri, "Diffusion and Effects of Cyber-Crime," 1057.
6. Some donors have established models for cybersecurity capacity building (CCB); for an overview see Muller, *Capacity Building in Developing Countries*. 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, *Capacity Building: Developing Access*, 5.
7. In total, 175 countries were represented, together with international organisations, the 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.
8. Klimburg, *The Darkening War*, 326, describes the three main policy dimensions of cyberspace: (1) the international peace and security dimension; (2) the economic, development and crime dimension; and (3) the Internet governance dimension. The scope of the present article does not allow me to contribute to the literature on Internet governance, although it overlaps with the second dimension. See Drake and Price, *Internet Governance – The NETmundial Roadmap*; Weber, *Shaping Internet Governance*; Balleste, *Internet Governance*; Kleinwachter, *Power of Ideas*; Shackelford and Craig, "Beyond the New 'Digital Divide'"; and Kulesza, "International Internet Law."
9. WSIS, *Outcome Document of the High-Level Meeting*, point 17. See also Global Commission on Internet Governance, "One Internet"; World Bank, *World Development Report 2016*; Bildt, *Development's Digital Divide*.
10. UN, *General Assembly's Overall Review*, 7; McKinsey & Company, "Offline and Falling behind," 2.
11. See WSIS, *Outcome Document of the High-Level Meeting*; WSIS, *Advancing Sustainable Development*, point 4.
12. Bildt, *Development's Digital Divide*.
13. See studies for Myanmar: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Myanmar.pdf, and for Tanzania: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Tanzania.pdf
14. Klimburg and Zylberberg, *Capacity Building: Developing Access*, 10.
15. World Bank, *World Development Report 2016*.
16. A bot.net consists of many Internet-connected computers where components communicate and coordinate actions that can be used to send spam email or distributed denial-of-service (DDOS) attacks. A bot herder or a botnet herder is a person who controls and maintains a botnet by installing malicious software in numerous machines, which can be controlled and used to attack or infect other machines.
17. Sullivan, "Who's behind Criminal 'Bot' Networks?"
18. Kshetri, "Diffusion and Effects of Cyber-Crime," 1071.
19. Cuellar, "Mismatch between State Power and State Capacity."
20. Gady, "Africa's Cyber WMD."
21. Palmer, "Rogue States Play Host"; Goncharov, *Criminal Hideouts for Lease*.
22. Landau, *Surveillance or Security*.
23. Timberg, "German Researchers Discover a Flaw."
24. See for instance Wagley, "Telecom Investments Threaten Privacy Rights"; and Langø, *Capacity Building: Security and Freedom*, 18–9.
25. For an overview of models measuring cyber-capacity maturity in the Global South, see Muller, *Capacity Building in Developing Countries*, 7–10.
26. See for instance ITU, *Impact of Broadband on the Economy*; World Bank, *World Development Report 2016*.
27. Dalberg, *Impact of the Internet in Africa*, 9; Klimburg and Zylberberg, *Capacity Building: Developing Access*.
28. UNGA A/70/174 (2015), 11.
29. Because there is 'no guarantee that the future evolution of the cyber-regime complex will occur in a manner conducive to Internet stability and global interoperability, the "responsibility to troubleshoot" (R2T) is an important hedge against the significant costs associated with cyber disruption' Raymond claims (Raymond, *Managing Decentralized Cyber Governance*).

30. Director for the National Cybersecurity Center in Myanmar, interview, October 2016.
31. See infographic on Tanzania's mobile money revolution: http://www.cgap.org/data/infographic-tanzanias-mobile-money-revolution
32. Mbogo, "Impact of Mobile Payments," 182–203; Bright and Hruby, "Rise of Silicon Savannah."
33. Tafirenyika, "Information Technology Super-Charging."
34. Dusabirane, "East Africa: Airclerk's CEO."
35. Digital in Asia, "Myanmar 22 Million Mobile Users, Smartphone Usage 80%," accessed October 17, 2017, https://digitalinasia.com/2017/01/09/myanmar-33-million-mobile-users-smartphone-usage-80
36. di Castri, *Mobile Money*.
37. This point, made by Kshetri, seems relevant to mention here, but the scope of this article does not allow me to go into a deeper discussion about bandwidths. For those particularly interested in the topic, I recommend Kshetri's article, "Will Blockchain Emerge as a Tool," 1720–1.
38. Global Commission on Internet Governance, "One Internet."
39. World Bank, *World Development Report 2016*, 16.
40. Various methodological models for fostering more efficient cybersecurity capacity building have been developed; for an overview, see Klimburg and Zylberberg, *Capacity Building: Developing Access*, 20–6; and Muller, *Capacity Building in Developing Countries*.
41. World Bank, *World Development Report 2016*, 205.
42. ASPI, Cyber-Maturity Report.
43. World Bank, *World Development Report 2016 – Digital Dividends*.
44. Calderaro, "Internet Governance Capacity Building in Post-Authoritarian Contexts."
45. ASPI, Cyber-Maturity Report.
46. World Bank, *World Development Report 2016*, 219.
47. Ibid., 208.
48. Klimburg and Zylberberg, *Capacity Building: Developing Access*, 9.
49. Ibid.
50. World Bank, *World Development Report 2016*, 255.
51. Wong and Solon, "Massive Ransomware Cyber-Attack Hits Nearly 100 Countries Around the World."
52. Statcounter, *Desktop Windows Version Market Share Europe.*
53. See for instance the Global Forum of Cyber Expertise's Dehli Communique on a GFCE Global Agenda for Cyber Capacity Building, 2017.

Bibliography

ASPI (Australian Strategic Policy Institute) Cyber-Maturity Report, 2016. https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf

Balleste, Roy. *Internet Governance: Origins, Current Issues, and Future Possibilities*. Lanham, MD: Rowman and Littlefield, 2015.

Bildt, Carl. *Development's Digital Divide*. Project Syndicate, 2015. Accessed August 15, 2017. http://www.project-syndicate.org/commentary/sustainable-development-goals-digital-divide-by-carl-bildt-2015-08

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

Calderaro, Andrea. "Internet Governance Capacity Building in Post-Authoritarian Contexts." *Telecom Reform and Human Rights in Myanmar*, 2016. Available at SSRN: https://ssrn.com/abstract=2686095 or https://doi.org/10.2139/ssrn.2686095

di Castri, Simone. *Mobile Money: Enabling Regulatory Solutions*. GSMA Mobile Money for the Unbanked, 2013. Available at GSMA: https://www.gsma.com/publicpolicy/wp-content/uploads/2013/02/GSMA2013_Report_Mobile-Money-EnablingRegulatorySolutions.pdf

Cavelty, Myriam Dunn. "Cyber-Security and Private Actors." In *The Routledge Handbook of Private Security Studies*, edited by Rita Abrahamsen and Anna Leander, 89–99. New York: Routledge, 2016.

Cuellar, Mariano-Florentino. "The Mismatch between State Power and State Capacity in Transnational Law Enforcement." *Berkeley Journal of International Law* 22, no. 1 (2004): 15–58.
Dalberg. *Impact of the Internet in Africa: Establishing Conditions for Success and Catalysing Inclusive Growth in Ghana, Kenya, Nigeria and Senegal*, 2013. Accessed March 18, 2016. http://www.impactoftheinternet.com/pdf/Dalberg_Impact_of_Internet_Africa_Full_Report_April2013_vENG_Final.pdf
Drake, William J., and Monroe Price, eds. *Internet Governance – The NETmundial Roadmap*. Los Angeles, CA: USC Annenberg Press, 2014.
Dusabirane, David. "East Africa: Airclerk's CEO Envisions a Cashless Economy in Rwanda." *All Africa*, 2015. Accessed August 15, 2017. http://allafrica.com/stories/201511050868.html
Gady, Franz-Stefan. "Africa's Cyber WMD." *Foreign Policy* (2010). Accessed August 15, 2017. http://foreignpolicy.com/2010/03/24/africas-cyber-wmd/
Global Commission on Internet Governance. "One Internet." 2016. https://www.cigionline.org/publications/one-internet
Goncharov, Max. *Criminal Hideouts for Lease: Bulletproof Hosting Services*, Trend Micro report, 2015. Accessed August 15, 2017. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-criminal-hideouts-for-lease.pdf?_ga=1.24160381.61042644.1458131160
ITU (International Telecommunication Union). *Impact of Broadband on the Economy*. 2012. Accessed August 15, 2017. https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf
Kleinwachter, Wolfgang. *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment*. Berlin: Marketing fur Deutschland GmbH, 2007.
Klimburg, Alexander. *The Darkening Web – The War for Cyberspace*. New York: Penguin Press, 2017.
Klimburg, Alexander, and Hugo Zylberberg. *Cyber Security Capacity Building: Developing Access*. NUPI Report no. 6. Oslo: Norwegian Institute of International Affairs, 2015.
Kopytoff, Igor, ed. *The African Frontier – The Reproduction of Traditional African Societies*. Bloomington: Indiana University Press, 1987.
Kshetri, Nir. "Diffusion and Effects of Cyber-Crime in Developing Economies." *Third World Quarterly* 31, no. 7 (2010): 1057–1079.
Kshetri, Nir. *Cybercrime and Cybersecurity in the Global South*. New York: Palgrave Macmillan, 2013.
Kshetri, Nir. "Will Blockchain Emerge as a Tool to Break the Poverty Chain in the Global South?" *Third World Quarterly* 38, no. 8 (2017): 1710–1732.
Kulesza, Joanna. "International Internet Law." *Global Change, Peace & Security* 24, no. 3 (2012): 351–364.
Landau, Susan. *Surveillance or Security – The Risks Posed by New Wiretapping Technologies*. Cambridge, MA: MIT Press, 2010.
Langø, Hans Inge. *Cyber Security Capacity Building: Security and Freedom*, NUPI Report no. 1. Oslo: Norwegian Institute of International Affairs, 2016.
Mbogo, Marion. "The Impact of Mobile Payments on the Success and Growth of Micro-Business: The Case of M-Pesa in Kenya." *Journal of Language, Technology & Entrepreneurship in Africa* 2, no. 1 (2010): 182–203.
McKinsey & Company. "Offline and Falling behind: Barriers to Internet Adoption." 2014. Accessed August 15, 2017. http://www.mckinsey.com/industries/high-tech/our-insights/offline-and-falling-behind-barriers-to-internet-adoption
Muller, Lilly Pijnenburg. *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*. NUPI Report no. 3. Oslo: Norwegian Institute of International Affairs, 2015.
Palmer, Maija. "Rogue States Play Host to Outlaw Servers." *Financial Times*, March 16, 2016. Accessed August 15, 2017. http://www.ft.com/intl/cms/s/2/c926b4ec-da25-11e5-98fd-06d75973fe09.html#axzz434Bv3Q84
Raymond, Mark. "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot." *Strategic Studies Quarterly* 10, no. 4 (2016): 123–149.
Shackelford, Scott, and Amanda Craig. "Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity." *Stanford Journal of International Law* 50 (2014): 119–185.
Statcounter. 2017. "Desktop Windows Version Market Share Europe May 2016 – May 2017." http://gs.statcounter.com/os-version-market-share/windows/desktop/europe/#monthly-201605-201705

Sullivan, Bob. "Who's behind Criminal 'Bot' Networks?" 2007. Accessed August 15, 2017. http://www.unl.edu/eskridge/cyberbot3.htm

Tafirenyika, Maimba. "Information Technology Super-charging Rwanda's Economy." *Africa Renewal*, 2011. Accessed August 05, 2017. http://www.un.org/africarenewal/magazine/april-2011/information-technology-super-charging-rwandas-economy

Timberg, Craig. 2014. "German Researchers Discover a Flaw That Could Let Anyone Listen to Your Cell Calls." *Washington Post*, December 18, 2014. Accessed August 15, 2017. 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/

UN. *United Nations General Assembly's Overall Review of the Implementation of WSIS Outcomes,* 2015. Accessed August 15, 2017. http://www.un.org/pga/70/wp-content/uploads/sites/10/2015/08/2015_October_09_World-Summit-on-Information-Society.pdf

Wagley, Rachel. "Telecom Investments Threaten Privacy Rights in Burma." *US Campaign for Burma*, 2014. Accessed August 15, 2017. https://uscampaignforburma.wordpress.com/2014/02/04/telecom-investments-threaten-privacy-rights-in-burma-2/

Weber, Rolf H. *Shaping Internet Governance: Regulatory Challenges*. Berlin: Springer-Verlag, 2010.

Wong, Julia Carrie, and Olivia Solon. "Massive Ransomware Cyber-Attack Hits Nearly 100 Countries Around the World." *The Guardian*, 2017. https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs.

World Bank. *World Development Report 2016 – Digital Dividends*, 2016. Accessed August 15, 2017. http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf

WSIS (World Summit on the Information Society). *Advancing Sustainable Development through Information and Communication Technologies: WSIS Action Lines Enabling SDGs*, 2015a. Accessed August 15, 2017. https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_booklet.pdf

WSIS (World Summit on the Information Society). *Outcome Document of the High-level Meeting of the General Assembly on the Overall Review of the Implementation of WSIS Outcomes*, 2015b. Accessed August 15, 2017. http://workspace.unpan.org/sites/Internet/Documents/UNPAN95707.pdf