Walter Leal Filho
,
Anabela Marisa Azul
,
Luciana Brandli
,
Amanda Lange Salvia
and
Tony Wall
Industry, Innovation and Infrastructure
Encyclopedia of the UN Sustainable Development Goals
10.1007/978-3-319-71059-4_115-1

Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries

Niels Nagelhus Schia[1] and Ole Johan Willers[1]

(1)Norwegian Institute of International Affairs [NUPI], Oslo, Norway

Niels Nagelhus Schia (Corresponding author)
Email: nns@nupi.no

Ole Johan Willers
Email: willers@nupi.no

Without Abstract

Synonyms

Cyber frontier; Cybersecurity; Cybersecurity capacity building; Digital dividends; Digital pitfalls; Digitalization; Sustainable Development Goals, SDGs

Definition

How does digitalization lead to new kinds of global connections and disconnections in the developing countries? And which role does digitalization play for the UN's Sustainable Development Goals? This entry focuses on cybersecurity capacity building (CCB) and the sustainability of development processes in developing countries.

Dividends and Vulnerabilities

New information and communication technologies (ICT) 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 been confirmed through statistics on the use of information technology, and the extent to which countries are connected correlates with increases in GDP (World Bank *2016*, p. 3). Donor countries and international organizations seize on digitalization as an opportunity to fight poverty.

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 have to be dealt with before most people in developing countries can enjoy extensive use of the Internet. 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 ITU *2012*; World Bank *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. Traditional development policy and projects might, therefore, become central elements for bridging the digital divide.

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 on the one hand, and digital vulnerability and cyber security in developing countries on the other (See: https://www.itu.int/net4/wsis/sdg/Content/wsis-sdg_booklet.pdf and http://workspace.unpan.org/sites/Internet/Documents/UN-PAN95707.pdf in particular bulletpoint 4).

Developing countries are implementing digital solutions and increasing digital connectivity at a rapid pace. The potential for economic and societal growth is enormous. However, the trend toward digitally enabled growth also creates digital vulnerabilities and risks that need to be addressed. Cyber capacity building is the process that covers these efforts. How does digitalization lead to new kinds of vulnerabilities in the Global South, and how are they relevant for the Sustainable Development Goals? This entry sets out to explore how these questions have been discussed in extant literature about cybersecurity capacity building in the Global South and identifies areas in need of more research and attention.

Cyber Capacity Building and Digital Development

Digital development is a key driver of economic and societal growth in the Global South. Increased connectivity and access to digital solutions can help public administrations to provide better services and provide improved business opportunities resulting in faster economic growth and more jobs (World Bank *2016*).

Digitalization also affects how donor countries can contribute assistance to sustainable development and to help achieve the Sustainable Development Goals. There is broad consensus about the importance of connecting developing countries to digital networks, so as not to widen the gaps between rich and poor states (Heeks *2014*; Principles for Digital Development *2019*; World Bank *2008*). Digital technology and connectivity are a cornerstone in almost every societal sector such as business and trade, communication and information, and education and health. But at the cyber-frontier, new types of vulnerabilities emerge (Schia *2018*). Developing countries often have low levels of regulatory capacity and are therefore especially vulnerable to exploitation. Cyber Security Capacity Building (CCB) seems set to play an increasingly important role in future foreign policy considerations and government programs (Schia *2016*).

CCB can be understood as an "umbrella concept for all types of activities (e.g. human resources development, institutional reform or organisational adaptations) that safeguard and promote the safe, secure and open use of cyberspace" (Pawlak *2014*). Alexander Klimburg and Hugo Zylberberg define CCB as pursuing a threefold aim: First, to provide a foundation for developing countries to reap digital dividends as access to cyberspace has become essential to social, economic, and political stability; second, to strengthen the global security landscape by limiting the number of safe havens for cybercriminals. Developing countries are increasingly becoming hosts to the infrastructure and actors behind malicious cyber activities. Bridging the digital divide is therefore important also with regard to responding to national security and various types of cyber threats in donor countries. And third, to advance and promote a model of digital governance that is rooted in the notions of openness, freedom, and security, which has become increasingly important as 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.

International Mandate and Relation to the Sustainable Development Goals

Whereas digital development became an increasingly prominent feature of development work throughout the 2000s (Heeks *2002*, *2010*; World Bank *2008*), digital vulnerabilities and risks were typically not included systematically in these efforts.

In 2010, the United Nations' Group of Governmental Experts (UN GGE) recognized cyber capacity building as being of "vital importance to achieve success in ensuring global ICT security, to assist developing countries in their efforts to enhance the security of their critical national information infrastructure, and to bridge the current divide in ICT security" (United Nations *2010*). The subsequent 2013 report linked this voluntary measure to "contribute to the achievement of Millennium Development Goal 8, to "develop a global partnership for development""(United Nations *2013*). The most recent 2015 report reiterated the importance of CCB and doubled the scope dedicated in the final document (United Nations *2015*). Despite the prominence of CCB throughout the GGE reports, cybersecurity has yet to be addressed systematically in the Security Council. None

of the permanent members have brought cyber to the UNSC, and other countries – for instance, Lithuania and the Netherlands – have considered introducing cybersecurity issues in the Council, but no action has followed. One recent members-elect, Estonia, raised the issue and organized an Arria meeting in May 2020 to discuss it (Tikk and Schia *2020*).

Nonetheless, CCB has received increasing awareness from international organizations. For example, the OECD emphasized "a need for better alliances and partnerships with like-minded countries or allies, including facilitating capacity building of less developed countries" (2012, p. 13), and the Principles for Digital Development recognize privacy and security as fundamental building blocks of digital development projects (Principles for Digital Development *2019*). Consequently, it is expected that CCB will develop into "one of the most important activities within the security/development nexus" (Klimburg and Zylberberg *2015*, p. 5).

CCB has thus become a recognized issue of concern both within international politics more broadly as an essential component to foster the resilience and security of digital technologies, and as a central aspect for digital development. Robert Morgus concludes that "[t]echnology can aid in the attainment of every SDG. But in order to fully reap the immense benefits of connectivity and digitalization, the technology that underpins it must be secure and the people that use it must understand how to do so responsibly and securely" (Morgus *2018*, p. 13). CCB is hence not an end in itself. Rather, it is a cross-cutting concern across all SDGs.

Whereas the 2010 UN GGE Report highlighted the importance of CCB for international cooperation and partnership (MDG 8), reliable and secure digital technologies are equally crucial as a factor contributing to economic growth and ending poverty and hunger (SDG 1 & 2) (Qiang et al. *2009*; World Bank *2008*). Thereby, Internet access and digitalization can afford more people to enjoy decent working conditions and increased income (SDG8) and boost innovative capacity with few requirements for expensive initial investments (SDG 9). Digital solutions can give access to more and better health services (SDG 3) and improve educational opportunities around the globe (SDG 4). Further, as water and energy supplies (SDG 6 & 7) are increasingly digitalized, the reliability and quality of access depend increasingly on the ability to secure the underlying critical information infrastructure, often in the form of public-private partnerships (Kvochko *in* Pawlak *2014*, p. 43). Additionally, immediate access to information provides an important layer of public control and scrutiny to political institutions, holding institutions to account and driving peace and justice (SDG 16). Responsible use of digital technologies is of outmost importance, and states in the Global North and South need to develop international norms and practices that ensure that digital technologies are not used to suppress and survey domestic opposition and activists, and to ensure a free and open Internet.

Digital Risks in the Global South

Digitalization is not simply a matter of joining cyberspace: It is a question of selective forms of global connection in combination with disconnection and exclusion. The trajectory of digitalization in the Global South diverges in various ways from that of more industrialized countries. As relative late adapters of digital technologies, developing countries engage in "technological leapfrogging," which in turn is interlinked with the risk of new and unprecedented societal vulnerabilities. This risk results from the lag between technology development, on the one hand, and societal capacity and management of this technology, on the other hand, characterized by scholars as a societal

"hollowness" caused by rapid digitalization processes (Kshetri *2010*, p. 153). This hollowness refers to weak or inadequate institutions, policies and strategies, poor organizational and individual defense 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.

Many developing countries have no published, officially recognized national cybersecurity strategies, or designated overarching units or institutions to coordinate national cybersecurity (Schia *2018*). Additionally, many of these countries also lack institutions to oversee and protect their digital critical infrastructure and thus also formal collaboration between the government and owners of critical assets. The governments' focus is often on becoming digital, and cybersecurity is not their priority right now.

This has implications for the ability of developing countries to address cybercrime and protect national critical infrastructure against digital attacks. Cybercriminals often deliberately operate through jurisdictions with low or nonexisting cybercrime legislation, making use of jurisdictional arbitrage to avoid legal consequences for their malicious action. As cybercrime is transnational, low regulatory capacity in developing countries can produce negative ramifications even in the most advanced digital economies. For example, Internet scamming and fraud originate overwhelmingly in regions with low cyber enforcement capability such as Nigeria. The Budapest Convention on Cybercrime provides a framework to harmonize national laws in order to prevent cybercriminals from operating with impunity. Developing countries have, however, been slow to sign on to the convention and often lack the necessary law enforcement capacity to enforce the legislation. Peters and Jordan (*2019*) argue that global awareness about the importance of capacity building for cybercrime has not translated into political will among donor countries. Consequently, they conclude, the global enforcement gap remains largely unaddressed as technical, operational, and strategic capabilities are lacking.

Leapfrogging digital technologies have also implications on the infrastructure of connectivity in the Global South. Digital connectivity can be divided into three aspects – often referred to in terms of the World Bank's "three miles" approach: 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 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. 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 kilometers of undersea broadband cables along the coasts of East Africa (e.g., SEACOM) and West Africa (e.g., 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. Nonetheless, many developing countries rely on very few or just a single Internet Exchange Point (IXP), connecting the country to the global Internet infrastructure. These countries are particularly vulnerable to disruption and governmental control as all data traffic in and out the country flows through a single gateway (Schia *2018*).

The middle mile refers to the national Internet backbone and intercity networks. The quality of these often depends 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. Liberalizing the market for the middle mile is an effective way of providing open access 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" (Schia *2018*).

A crucial difference to developed countries is that in the Global South, the last mile is rarely served through fixed copper cables. Instead, local access to networks is dominated by wireless alternatives. Whereas the Global North had achieved almost universal fixed-line access before wireless technology was introduced, most countries in the Global South have never built fixed-line networks. This has severe consequences for the usage and performance of Internet access. Wireless networks tend to be more expensive and rarely offer flat-rate pricing and offer slower speeds. Hence, the World Bank concludes that "many developing countries are stuck with a second-class internet that may fail to deliver the expected benefits, especially for business users" (World Bank *2016*, p. 208). Slow Internet connections can also be a security risk. For example, distributed denial of service (DDOS) attacks are more difficult to mitigate as occurred in Myanmar during the run-up to the 2010 general elections.

Types of CCB Projects

CCB includes a range of projects with the aim to address digital risks in recipient countries. These can be divided into five overarching thematic categories: policy and strategy; culture and society; education and skills; regulation; and standards (Bellasio et al. *2018*). The Global Cyber Security Capacity Centre at the University of Oxford has developed the "Capacity Maturity Model (CMM)" to assess a nation's current capacity and needs across these five categories (Global Cyber Security Capacity Centre *2016*). Policy and strategy projects are concerned with the development of national cybersecurity strategies, incident response teams, critical infrastructure protection, crisis management, defense capability, and crisis redundancies. Projects with a cultural and societal focus aim to improve public knowledge about reporting mechanisms and privacy rights. Educational projects target both the population at large through awareness-raising campaigns and develop programs to train qualified specialists locally. Legal and regulatory projects support recipient countries with the development and implementation of legal frameworks to, for example, curb cybercrime. Last, projects with a standard dimension promote adherence to international standards such as cryptographic protocols and technical security controls.

However, focusing on a whole-of-society approach implies a risk of implementing too fragmented efforts to cybersecurity capacity building. This risk has been raised by scholars such as Calandro and Berglund who make the point that a lack of coordination between CCB actors may undermine the success of such projects. If this could be overcome, CCB could exert greater influence on cyberspace governance than the development of international treaties (Calandro and Berglund *2019*).

Actors in CCB

CCB projects include typically three actor categories: funders, recipients, and implementers. A national or international funding agency provides the resources to finance a given project. It is not uncommon that these are different from national development agencies. For example, Patryk Pawlak and Panagiota-Nayia Barmpaliou observe that the diplomatic and law enforcement agencies dominate the CCB community (Pawlak and Barmpaliou *2017*). Further, it has been argued that "as

the risks and the security environment evolve, traditional development actors no longer hold the monopoly or are well-equipped to provide the support required. Consequently, other actors – including the military and law enforcement agencies – are forced to step in" (Pawlak *2017*). In addition to funding, methodological, technical, and infrastructure support is often provided (Morgus *2018*).

The second actor type is the recipient state or region that receives this funding based on an agreed project design. Oftentimes, CCB projects have a regional scope as, for example, the S3SA project, covering the Southern African region. Other projects are global in outlook but target individual countries for specific projects such as the World Bank's Global Cybersecurity Capacity Building Program that covered countries in the Western Balkan, Western Africa, and Central Asia (World Bank *2019*).

The third actor type covers those organizations that implement projects and provide technical assistance. A range of consultancy firms provide technical expertise to assist recipient states in the development of national strategies, educational programs, and protection of critical infrastructure. There is significant variation among implementing consultancy firms. Small and specialized consultancies are typically contracted for clearly defined project areas. Globally operating large consultancies on the other hand can be contracted for entire projects, steering the implementation across different project layers and regions. The World Bank's Global Cybersecurity Capacity Building Program relied, for example, for the entire project period across regions on a consortium of Deloitte and the Telecom Strategy Consultants (World Bank *2019*). In addition to consultancies, academic and nongovernmental institutions can take on roles within the implementation process. Like funding agencies, these actors can provide methodological and technical support and are often critical actors for the identification of needs in recipient states and to organize stakeholder consultations.

There are, however, a range of other actors involved in CCB projects. International organizations such as the Organization for Security and Cooperation in Europe (OSCE), the United Nations Office on Drugs and Crime (UNODC), the International Telecommunications Union (ITU), and Interpol all play their part in facilitating capacity-building projects. An important part of their work is to provide best-practice guidance such as the ITUs "Digital Identity Roadmap" or the multistakeholder "Guide to Developing a National Cybersecurity Strategy." The Global Forum for Cyber Expertise (GFCE) represents an additional actor with the aim to facilitate coordination among the multiple CCB actors. Funded by the United Kingdom and the Netherlands in 2015, the GFCE brings together public officials, international organizations, development agencies, research institutes, and private companies to facilitate the development of a global agenda for CCB and avoid duplications of efforts (GFCE *2015*).

Dilemmas of CCB

Several scholars have noted that development agencies have been slow in addressing digital risks (Hohmann et al. *2017*; Morgus *2018*). Located at the nexus between security and development work, several dilemmas have plagued efforts to disseminate cybersecurity capacity.

The EU Operational Guidance on Cybersecurity Capacity Building discusses several of these dilemmas (Pawlak *2018*, pp. 41–46). First, cybersecurity efforts often face – if only indirect – questions about the balancing of security and human rights. Encryption illustrates this dilemma.

Affording citizens an additional layer of precaution to prevent unauthorized access to information, encrypted communication frustrates the work of law enforcement and intelligence services. A more general concern is the dual-use nature of cyber capabilities: "the difficulty in constraining the potential misuse of equipment or skills delivered for purely defensive purposes weighs heavily on decisions to provide assistance" (Pawlak *2017*, p. 2). The fear is that the capacity, once disseminated, is out of control of the donor state and might be used for purposes that undermine the human rights situation in the recipient state.

A second dilemma is identified in relation to the reconciliation of differing and at times contradictory ideas about sovereignty, legitimacy, and approaches to Internet governance. The past years have seen a growing conflict over the Internet governance model. On the one hand, many Western countries advocate for a continued decentralized multistakeholder model with limited authority for state actors. On the other hand, an alliance of countries led by China and Russia favors an approach rooted in national sovereignty with a greater emphasis on state responsibilities to control and if necessary limit the flow on information. The increasing tension over questions of governments' role and legitimacy has led Alexander Klimburg to proclaim the "Yalta Moment," marking the start of a "cold war for internet governance" (Klimburg *2013*). With many developing countries holding a swing-state position on this issue, this dilemma clearly speaks to the geopolitical dimension of CCB. A related dilemma relates to the domestic governance of law enforcement and intelligence services, requiring a balancing of oversight and transparency. Too much transparency constrains operational effectiveness, but too little oversight provides a fertile ground for misuse and overreach of mandate.

Challenges to CCB

Adding to these inherent dilemmas in capacity building, CCB also faces challenges that are more closely linked to the nascent nature of this policy issue. Among these is a challenge to coordinate between stakeholders to avoid a duplication of efforts; a need for better integration among stakeholders to facilitate learning across policy communities and ensure project success; a shortage of implementers; the importance of locating local partners; and a shortage of funding.

The coordinative challenge weighs heavily on CCB. Early efforts have resulted in a fragmented coverage of CCB and unnecessary duplications of effort (Hohmann et al. *2017*; Pawlak *2014*, p. 17; Pijnenburg Muller *2015*, p. 7). The Global Forum for Cyber Expertise was established to facilitate a more coordinated approach, bringing stakeholders across the globe together and acting as a clearing house for CCB projects. Relatedly, because CCB projects often include stakeholders from various policy communities – spanning technical, law enforcement, diplomatic, and development sectors – coordination between actors needs to cross sectors and knowledge structures, constraining systematic learning and project evaluations. Given the diversity of actors involved, CCB projects are not merely technical processes. Instead, Pawlak and Barmpaliou argue that CCB is "charged with political assumptions and objectives," sometimes resulting in clashing ideologies, and note the rise of the "politics of CCB" (Pawlak and Barmpaliou *2017*). Zine Homburger shows how this goes beyond the focus on western states and addresses CCB efforts of China and Russia (*2019*).

A direct example of clashing ideologies is the poorly integrated development community in CCB efforts (Klimburg and Zylberberg *2015*; Morgus *2018*; Pawlak and Barmpaliou *2017*). "Most experts point to development actors' uneasy relationship with cyber *security* capacity building. […] Moving

forward, the technical expertise of cybersecurity professionals should ideally be integrated with the procedural experience on capacity building in the development community" (Hohmann et al. *2017*, p. 23). Without the enrollment of the development community, it is more difficult to identify local project partners and create project ownership and avoid supply-driven project designs – a central factor in ensuring the long-term sustainability of capacity-building projects (Eade *1997*). A third challenge has been a general lack of implementers (Pijnenburg Muller *2015*), which can be traced back both to a global shortage of cyber experts and to a lack of funding opportunities within CCB. Morgus (*2018*) estimates global annual CCB funding to be in the "range from roughly US$50 million to roughly US$1 billion, with the mean estimate far closer to the lower end of that spectrum." (p. 29). One important factor constraining higher funding levels has historically been uncertainty as to the qualification of CCB projects as development aid within the DAC guidelines and hence contributing to a donor country's official development assistance (Hohmann et al. *2017*; Klimburg and Zylberberg *2015*). Private sector actors face thus little incentive to invest into the nascent field of CCB.

While the discussed challenges have had major influence on the hitherto development of CCB as a key issue within the security/development nexus, they can be mostly attributed to the emerging nature of the field.

Conclusion

This entry has drawn on the extant literature on cybersecurity capacity building in order to highlight connections between digitalization and the Sustainable Development Goals. New kinds of societal vulnerabilities are emerging, and new power relations are being forged. By emphasizing (trans)formation and continuity, we have shed light on the connections between digitalization, economic growth, and cybersecurity. This triple knot indicates a development where the "haves" can reap digital dividends, leaving the "have-nots" behind. The growing digitalization 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.

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 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.

Clearly, there is a potential for more focused and systematic scholarly research and data collection that could underpin donor countries and help to facilitate programs 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 are 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 has highlighted the technological, organizational, and human dimensions as well as the local, national, regional, and international levels of digitalization. Managing such challenges will require an in-depth understanding of the democratic, social, and economic development contexts on which cyberspace depends. 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. Donor countries can continue their long-term foreign policy traditions by incorporating a new policy field.

Cross-References

- Accessibility as a Precondition for Sustainable Development
- Development of New Skills
- Governance Innovation
- Innovation Networks
- Innovation Process and Product
- Risk-Based Approach to Sustainable Infrastructure
- Smart Cities
- Technological Solutions and Upgrade the Technological Capabilities
- Value Chain of Infrastructures
- Value Chain of Infrastructures (Construction Supply Chain)
- Vulnerability Assessments

References

Bellasio J, Flint R, Ryan N, Sondergaard S, Monsalve C, Meranto A, Knack A (2018) Developing cybersecurity capacity: a proof-of-concept implementation guide. RAND, Santa Monica. https://doi.org/10.7249/rr2072
CrossRef

Bildt C (2015) Development's digital divide. Project syndicate. http://www.project-syndicate.org/commentary/sustainable-development-goals-digital-divide-by-carl-bildt-2015-08

Calandro E, Berglund N (2019) Unpacking cyber-capacity building in shaping cyberspace governance: the SADC case

Dalberg (2013) Impact of the Internet in Africa: establishing conditions for success and catalysing inclusive growth in Ghana, Kenya , Nigeria and Senegal . http://www.impactoftheinternet.com/pdf/Dalberg_Impact_of_Internet_Africa_Full_Report_April2013_vENG_Final.pdf

Eade D (1997) Capacity-building: an approach to people-centred development. Oxfam, Oxford
CrossRef

GFCE (2015) Launch of the global forum on cyber expertise in The Hague Declaration on the GFCE

Global Cyber Security Capacity Centre (2016) Cybersecurity capacity maturity model for nations (CMM). Oxford

Heeks R (2002) Information systems and developing countries: failure, success, and local improvisations. Inf Soc 18(2):101–122. https://doi.org/10.1080/01972240290075039
CrossRef

Heeks R (2010) Do information and communication technologies (ICTs) contribute to development? J Int Dev 22(5):625–640. https://doi.org/10.1002/jid
CrossRef

Heeks R (2014) Future priorities for development informatics research from the Post-2015 development agenda. Development 57. https://doi.org/10.1016/0736-5853(84)90003-0

Hohmann M, Pirang A, Benner T (2017) Advancing cybersecurity capacity building implementing a principle-based approach. Global Public Policy Institute (GPPi), Berlin

Homburger Z (2019) The necessity and pitfall of cybersecurity capacity building for norm development in cyberspace. Glob Soc 33(2):224–242. https://doi.org/10.1080/13600826.2019.1569502

ITU (International Telecommunication Union) (2012) Impact of broadband on the economy. https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf

Klimburg A (2013) The Internet Yalta. Retrieved from https://s3.amazonaws.com/files.cnas.org/documents/CNAS_WCIT_commentary-corrected-03.27.13.pdf?mtime=20160906082142

Klimburg A, Zylberberg H (2015) Cyber security capacity building: developing access. Norwegian Institute of International Affairs, Oslo

Kshetri N (2010) Diffusion and Effects of Cyber-Crime in Developing Economies. Third World Quarterly 31(7):1057–1079

Morgus R (2018) Securing digital dividens – mainstreaming cybersecurity in international development

Pawlak P (2014) Riding the digital wave: the impact of cyber capacity building on human development. EUISS, Paris. https://doi.org/10.2815/43313
CrossRef

Pawlak P (2017) Building capacities for cyber defence. EUISS, Paris. https://doi.org/10.2815/379783
CrossRef

Pawlak P (2018) Operational guidance for the EU's international cooperation on cyber capacity building. European Union, Luxembourg. https://doi.org/10.2815/38445
CrossRef

Pawlak P, Barmpaliou P-N (2017) Politics of cybersecurity capacity building: conundrum and opportunity. J Cyber Policy 2(1):123–144. https://doi.org/10.1080/23738871.2017.1294610
CrossRef

Peters A, Jordan A (2019) Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. Journal of National Security Law & Policy 10: 487

Pijnenburg Muller L (2015) Cyber security capacity building in developing countries: challenges and opportunities. NUPI, Oslo

Principles for Digital Development (2019) Principles. Retrieved January 21, 2020, from https://digitalprinciples.org/principles/

Qiang CZ-W, Rossotto CM, Kimura K (2009) Economic impacts of broadband. In: Information and communications for development 2009: extending reach and increasing impact. World Bank, Washington, DC, pp 35–50

Schia NN (2016) Teach a person how to surf: Cyber security as development assistance. NUPI Report

Schia NN (2018) The cyber frontier and digital pitfalls in the global south. Third World Q 39(5):821–837. https://doi.org/10.1080/01436597.2017.1408403
CrossRef

Tikk E, Schia NN (2020) The role of the UN Security Council in cybersecurity: international peace and security in the digital age. In Tikk E and Kerttunen M (eds.) Routledge Handbook of International Cybersecurity. Routledge, London

United Nations (2010) A/65/201. United Nations, New York

United Nations (2013) A/68/98*. United Nations, New York

United Nations (2015) A/70/174. United Nations, New York

World Bank (2008) Global economic prospects – technology diffusion in the developing world. World Bank, Washington, DC
CrossRef

World Bank (2016) Digital dividends. In: World development report. World Bank, Washington, DC

World Bank (2019) Global cybersecurity capacity program – lessons learned and recommendations towards strengthening the program. The World Bank, Washington, DC