NEW AMERICA

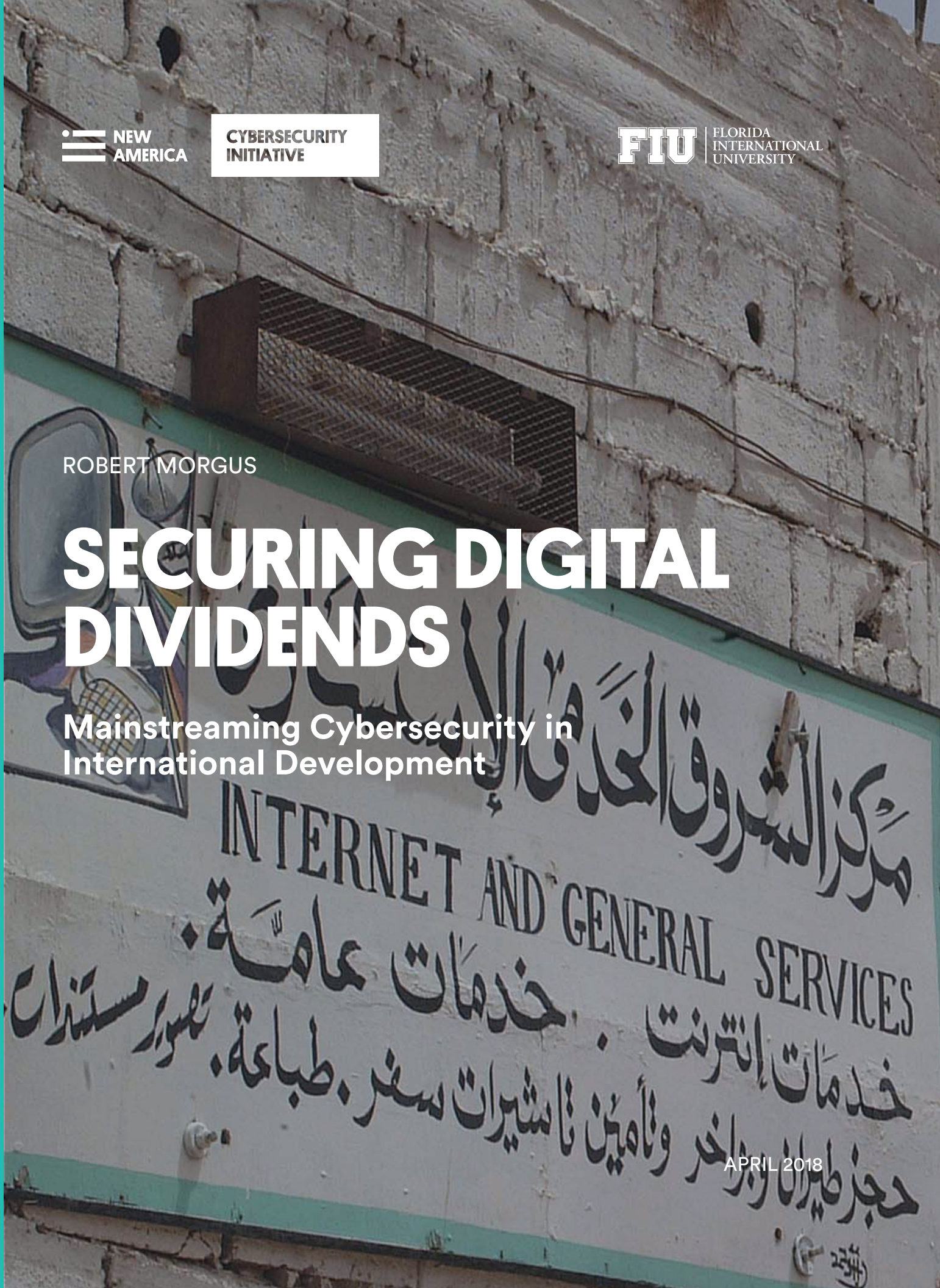
CYBERSECURITY INITIATIVE

FIU FLORIDA INTERNATIONAL UNIVERSITY

ROBERT MORGUS

SECURING DIGITAL DIVIDENDS

Mainstreaming Cybersecurity in International Development



APRIL 2018

NEW AMERICA

April 2018

Securing Digital Dividends

Mainstreaming Cybersecurity in International Development

Robert Morgus

Cybersecurity Initiative

Last edited on April 20, 2018 at 12:36 p.m. EDT

Acknowledgements

The author would like to thank Clementine Gazay, Emefa Agawu, Hande Guven, and Jiyeong Jeon for their research assistance, as well as Ian Wallace for acting as a sounding board and helping shape many of the ideas and insights in this report. In addition, the author owes a debt of gratitude to all the participants in the October 2017 workshop on Bridging a Critical Divide hosted at the UK Embassy in Berlin, Germany, as well as the experts and practitioners who carved time out of their busy schedules to contribute to this report through interviews and comments. This work is made possible through the generous support of the Florida International University, the William and Flora Hewlett Foundation, Microsoft Corporation, the Government of the United Kingdom, Endgame Inc., and the MITRE Corporation. The contents of this report to not necessarily reflect the views of those organizations or their employees. About the C2B Partnership: This paper was produced as part of the Florida International University - New America Cybersecurity Capacity Building Partnership (C2B Partnership). This innovative collaboration brings together two cutting edge institutions to address one of the biggest issues of our day: cybersecurity. Find out more at newamerica.org/cybersecurity-initiative/c2b/

About the Author(s)

Robert Morgus is a senior policy analyst with New America's Cybersecurity Initiative and International Security program and the deputy director of the FIU-New America C2B Partnership.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring the key attributes of New America's ethos to the cybersecurity policy conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. The Initiative seeks to address issues others can't or don't and create impact at scale.

Contents

Executive Summary

Introduction

Part I: The Case for Action

- Chapter 1: Cybersecurity in Development
- Chapter 2: Mainstreaming Cybersecurity

Part II: Understanding the Important Communities

- Chapter 3: Understanding Development
- Chapter 4: Understanding Cybersecurity Capacity Building
- Chapter 5: The Necessity of Bridging these Communities

Part III: Challenges and Solutions

- Chapter 6: Major Challenges to Mainstreaming
- Chapter 7: The Way Forward

Conclusion

Appendix: The SDGs and Cybersecurity

Executive Summary

Development underpinned by information and communication technologies (ICT) is unsustainable without acknowledging and taking steps to manage risks borne out of increased reliance on ICT. Without cybersecurity, ICT becomes a potential new point of failure that could threaten to undo development progress. As the development of economies, institutions, and society more broadly in lower- and middle-income countries becomes increasingly reliant on digital technologies, the imperative to do a better job of building capacity to manage digital risk increases.

The role of cybersecurity for the delivery of key development outcomes and the achievement of the Sustainable Development Goals is potentially immense, as much of the work to attain these outcomes is underpinned by information and communication technology. If this technology is untrustworthy and unreliable, countries and citizens may not fully reap the rewards of digitization. Worse yet, increased dependence on digital technology coupled with unreliability may threaten to actually create negative progress. Put simply, for technology to deliver on its immense promise, we must be able to trust the technology we use.

To help manage these risks in the lower- and middle-income parts of the world, a cybersecurity capacity building community of practice has developed across governments, industry, and civil society around the world. This community of practice, which shares many of the same goals as the development community, exists largely in isolation from the broader development community.

Given the nature of the cybersecurity challenge facing the developing world, cybersecurity must be mainstreamed in development in order to enable more resilient and sustainable development. The benefits of mainstreaming are numerous, from the delivery of more resilient development outcomes to improved development of cybersecurity capacity through shared expertise and experience.

In the face of these opportunities, four challenges exist. First, development donors—key stakeholders in the broader development community—are hesitant to fully embrace cybersecurity as a development issue. Second, in part due to the perceived complexity of cybersecurity, some recipients of development assistance—the stakeholders who largely drive the direction of spending—struggle to include cybersecurity in their development investment strategies. Third, because development spending can be perceived as zero-sum, money spent on cybersecurity could be seen as taking away from money potentially spent on alleviating other development stresses. Fourth, a general shortage of cybersecurity expertise globally means that finding affordable and willing expertise is difficult.

In response to these challenges, this report recommends a multifaceted approach to achieve both a strategic-level shift in the development community and prepare operators in the development community for success. Specific recommendations are:

- ***Reframe cybersecurity in the context of development*** by shifting discourse to "security for" instead of "security from"; reframing cybersecurity around risk management, resilience, sustainability, and trust; and creating more opportunities to communicate and collaborate.
- ***Build a library of credible and politically useful information to present to key development decision makers***, like deep statistical studies on the impact of cybersecurity on development and a library of case studies and examples of the positive and negative impacts of cybersecurity on key development outcomes.
- ***Demystify cybersecurity for aid recipients*** by identifying good practices in cybersecurity capacity building that are backed by rigorous empirics and developing a toolkit to enable bottom-up agenda setting.
- ***Bring more expertise into cybersecurity donor institutions*** by exploring short-term solutions like fellowships and secondments and leveraging funding mechanisms to create long-term cybersecurity portfolios in development donor institutions.
- ***Create and implement digital risk impact assessments for development projects and programs***, following a model similar to that of human rights or environmental impact assessments.

Introduction

At 3:35 P.M. local time on December 23, 2015, the heat clicked off in the eastern part of Ukraine. So did the lights. Three different distribution oblenergos (energy distribution companies) in eastern Ukraine had fallen prey to cyberattacks that resulted in "several outages that caused approximately 225,000 customers to lose power."[1] The details of the event are well covered, and those less familiar should refer to textbox 1.

Arguably, the problem in Ukraine started well before spring 2015 and the set of initial spear phishing emails. Most of the oblenergos in Ukraine underwent a process of privatization from the mid 1990s to the late 2000s.[2] With privatization came the realization that the grid's infrastructure was leading to inefficient and sometimes ineffectual power delivery. What followed in the early 2010s was a push to modernize Ukraine's power transmission system. The modernization consisted of replacing some analog equipment, like breakers, with newer analog equipment. However, some modernization efforts also introduced more automation and digitization of monitoring and control systems.[3] As Dejan Cerkic, a project manager who led grid modernization projects in Ukraine noted in 2012, "It is very important for a country like Ukraine to have a solid electrical system, because it is the basis of the economy." For Cerkic, "international projects, either with European investors or with the World Bank give an opportunity to modernize the transmission system faster than it can be done using local funds."[4]

Cerkic is right. This automation and digitization would enable more efficient delivery of power—from 19.71 percent power transmission lost in 2001 to 10.78 percent in 2014.[5] But the digitization of monitoring and control systems, combined with a destructive cocktail of insufficient local training on good computer hygiene, limited awareness of cyber threats, a lack of cybersecurity expertise, and limited implementation of technical solutions left the Ukrainian power grid open to new digital risks.

While the attacks on the Ukrainian power grid are perhaps the most visceral cyberattacks yet witnessed, Ukraine's power grid is not the only digital system vulnerable to exploitation. Incidents in low-, middle-, and high-income countries alike clearly communicate the inherent risks associated with digital systems. Global ransomware incidents WannaCry and NotPetya affected all nearly sectors in 150 and 65 countries respectively.[6] Liberia was taken offline entirely by cyberattacks.[7] Cybercrime in Nigeria has depressed foreign direct investment.[8] Cyber incidents in Bangladesh resulted in millions of dollars in theft.[9] Just as digitization holds great promise to improve the conditions of humans around the world, cyber risk threatens to erase progress or even worsen conditions.

The moral of these stories? It may not be what you think. Digitization is not bad—it is good. Digitization and connectivity yield unquestionable dividends and advance human development in ways that would have been unimaginable just a century ago. But the increased use of and reliance on digital systems simply carries with it new risks. As the development of economies, institutions, and society more broadly in lower- and middle-income countries becomes increasingly reliant on digital technologies, the imperative to do a better job of building local capacity to manage digital risk increases. The role of cybersecurity for the delivery of key development outcomes and the achievement of the Sustainable Development Goals is potentially immense, as much of the work to attain these outcomes is underpinned by trust in resilient information and communication technology. Without trust in and reliability of this technology, countries and citizens will not fully reap the rewards of digitization.

Cyber insecurity is an issue simultaneously impacting human security, economic stability, and society more broadly. As development institutions seed projects to digitize greater portions of society in the hope of improving conditions around the world, little attention is paid to building cybersecurity capacity—the capacity countries need to better manage these novel risks. A community—not dissimilar to the established development community—focused on building cybersecurity capacity exists. This cybersecurity capacity building community is a loose community of practice consisting of government agencies (from ministries of foreign affairs to ministries for development and telecommunication regulators), intergovernmental organizations, nonprofit/nongovernmental organizations, and private companies. These organizations work together and separately to grow human, technical, and organizational capacity to manage and combat cyber risk.

Despite its related goals, the cybersecurity capacity building community is largely disconnected from the development community. There are a number of reasons for this division, some intentional, some accidental. Additionally, the work of the cybersecurity capacity building community is as of yet imperfect. However, the increased use of information and communication technology and digital devices as tools to deliver better development outcomes necessitates taking steps to mainstream cyber risk management and cybersecurity capacity building in development.

That is what this report is about.

The remainder of this report proceeds as follows. Chapter 1 introduces how cybersecurity contributes to better development outcomes and the achievement of the SDGs. Chapter 2 discusses the various ways in which cybersecurity could be incorporated in the development community. Chapters 3 and 4 provide overviews of the development and cybersecurity capacity building communities respectively. Chapter 5 explores the primary benefits of bridging the divide

between these two communities and Chapter 6 delineates the primary challenges to doing so. Finally, Chapter 7 outlines a roadmap for overcoming these challenges and recommends specific actions for policy and decision makers to take.

Because the primary goal of this report is to help provide a blueprint for bridging a gap between two different communities, its audience is mixed. This means that some sections and even entire chapters may be review material for some readers. The report has attempted to highlight these sections for the readers and provides guidance for how to choose your own adventure in the text.

For the many things this report is about, there are two important issues in the context of development and cybersecurity that this report is ***not*** about: (1) making the development community more cybersecure in its own operations and (2) identifying good practices in cybersecurity capacity building. Scholarship to address these topics is a pressing need and both merit greater study but fall outside the scope of this project.

→ BOX 1

What Happened in Ukraine?

It all started about six months prior to December 2015. "There were phishing emails sent out," says Robert M. Lee,[10] who was one of the lead investigators of the 2015 hack of the Ukrainian power grid. This means that operators at the oblenergos in eastern Ukraine were receiving emails about "a variety of different events going on in Ukraine." When grid operators opened up these emails, "a piece of malware called BlackEnergy3 was dropped to the system." BlackEnergy3 enabled "attackers to steal credentials—usernames, passwords, things like that—from the network," which they could then use to regain access to the company's computer networks. According to Lee, over the next six months, the attackers "spent that time researching and understanding the environment."[11]

Once attackers gained the needed knowledge of the Ukrainian grid's operating systems, they were able to use their stolen credentials to gain remote access. With this access, they opened up the necessary digital control systems, clicked a mouse a few times, and shut a series of breakers, turning off the power.[12]

But they were not done there. Anticipating the natural reaction of the grid operators, which would be to try to reboot their computer systems in an effort to regain control and turn the lights back on, the attackers also uploaded a common piece of malware called KillDisk to the systems. When the station

operators in Ukraine attempted to reboot their devices, KillDisk kicked in, "deleting all the files and deleting all the systems." This meant that, "while the operators are trying to recover, they're also dealing with the fact that all their systems have gone down."[13]

Ultimately, the 2015 cyber attack left more than 200,000 people without electricity for approximately three hours. But the effects of the attack lasted beyond those three hours, as the impact of the attack forced operators to switch to manual operation of portions of the grid, nullifying the positive progress of digitization of power delivery.[14] And it could have been much worse. In some parts of the world, digital systems lack manual backups. In still more parts of the world, the reliance on digital systems means that localities lack the humans and expertise necessary to operate critical systems manually, even if that is an option.

Part I: The Case for Action

The cybersecurity challenge in the developing world is of increasing importance. Cyber insecurity can challenge or even unwind progress in growing economies, improving governance and enhancing the quality of life of individuals more broadly. Given the pervasiveness of ICT to development, cybersecurity should be mainstreamed across the development community. In this part, we outline the case for cybersecurity in development and explain why mainstreaming cybersecurity across the development community will lead to better outcomes.

Chapter 1: Cybersecurity in Development

In 2016, the World Bank's World Development Report (WDR) *Digital Dividends*, a cardinal document in the development community that is often used to drive the strategy of the community as a whole, explicitly acknowledged the importance of cybersecurity as a concern for international development. For the first time in a WDR, the importance of managing digital risk was enumerated, as the report noted, "some of the perceived benefits of digital technologies are offset by emerging risks."[15] Today, 80 percent of World Bank projects have information and communications technology (ICT) as a fundamental component, and this number is only likely to increase in the future.[16] Despite recognition from the World Bank, donor institutions and the development community are not doing enough to address risks stemming from increased reliance on ICT. Likewise, many in the developing world have embraced digital technology, but not always in its most secure form.

Digital risk in lower- and middle-income countries is not new and was recognized by some early on. In fact, to help manage these risks, a burgeoning cybersecurity capacity building community emerged in the early 2010s. Patryk Pawlak of the EU Institute for Security Studies describes the work of this community—cybersecurity capacity building—as "an umbrella concept for all types of activities (e.g. human resources development, institutional reform or organizational adaptations) that safeguard and promote the safe, secure and open use of cyberspace."[17] For the better part of a decade, the focus of this activity has been on strengthening national capabilities, developing collective capability, and facilitating international cooperation and partnership in cybersecurity.[18]

The work of this community is integral to better and more sustainable development. Good cybersecurity enables growth in the users and uses of ICT. This increased use in turn helps to grow economies and wealth, increase transparency, and enable easier communication and greater information transfer. However, as the Internet Society (ISOC) notes, "Diminishing trust is a

challenge to the Internet. To protect the opportunities of the Internet, we have to counter diminishing trust."[19] The diminishing trust cited by ISOC is driven by poor cybersecurity. The Internet Governance Forum's (IGF) *Best Practices Forum on Cybersecurity* report further outlines why poor cybersecurity leads to diminished trust and ultimately diminishes the effectiveness of ICTs for development:

> Poor cybersecurity threatens the growth of ICTs and Internet Technologies. Poor cybersecurity exposes organisations and individuals to risks and attacks, and opens doors for ill-meaning parties to spy on actors or meddle with democratic affairs. In a more indirect way, a perception of insecurity creates distrust in ICTs and the Internet and a diminishing adoption of new technologies. Poor cybersecurity will reduce the use and effectiveness of these technologies, and thus limit the opportunities to help achieve the SDGs.[20]

Policymakers around the globe, and particularly in lower and middle-income countries, are "facing an important challenge today: How to fully embrace the digital revolution while, at the same time, ensuring the safety and security of their citizens."[21]

Later in this chapter, we provide examples for how cyber insecurity can impact development outcomes. More work is needed to identify the ways in which cyber insecurity stunts economic growth, leads to institutional instability, and decreases human security, but reliance on ICT for large swaths of society, the economy, and governance is unsustainable without acknowledging and managing the risks associated with the use of computers and computer networks. Lower- and middle-income countries, and by extension development projects, are not intrinsically immune to these risks.

Global cybersecurity incidents like the WannaCry and NotPetya ransomware outbreaks catalyzed heightened interest and investment in many resource-rich, higher-income countries. However, in much of the lower-income world—the part of the world where the digital economy is growing nearly two times as fast as in the higher-income world, the part of the world where developments in e-government and e-governance could have an outsized impact on the quality of human life—the importance of managing new risks of digitization has often been overlooked and could threaten to undo these advances.

Cybersecurity helps achieve sustainable development outcomes and the SDGs

The benefits of digital development have been the subject of entire reports. Here, rather than focusing on digital development writ large, we will explore how cybersecurity enables the sustainable and resilient delivery of development outcomes and—in some cases—delivers development outcomes on its own.

As the U.K.'s Department for International Development (DFID) notes, "digital technologies have the potential to revolutionise the lives of the poor, unlock development and prosperity, and accelerate progress towards global goals."[22] However, the 2016 WDR acknowledges that, although "digital technologies have boosted growth, expanded opportunities, and improved service delivery... their aggregate impact has fallen short and is unevenly distributed."[23] For the World Bank, the "emerging risks" associated with digital technologies may offset some of the "perceived benefits."[24]

The Sustainable Development Goals (SDGs) provide a set of goals around which the development community coalesces.[25] Digital development and ICT for development (ICT4D) are means through which many of these ends are pursued. Among these goals are efforts like attaining zero hunger, quality education, gender equality, decent work and economic growth, reducing inequality, building strong peace and justice institutions, as well as building resilient industry, innovation and infrastructure. What these goals have in common is that they all seek to improve human security, institutional stability, and economic stability and growth.

Technology can aid in the attainment of every SDG. But in order to fully reap the immense benefits of connectivity and digitization, the technology that underpins it must be secure and the people that use it must understand how to do so responsibly and securely. At the end of this report, we offer a table outlining the SDGs, some notable targets, and how good cybersecurity contributes to the goals and targets. For those interested, this chart can be found in the appendix. Instead of going through this exhaustive list here, we focus on how cybersecurity and insecurity impacts three crucial pillars of development: (1) the economy, (2) governance, and (3) human security, using the SDGs as a framing device where appropriate.

The economy

There is a good economic case for cybersecurity. Sustainable Development Goal #1, end poverty, targets to halve the number of humans living in poverty by 2030 and reduce inequality of economic opportunity.[26] Similarly, SDG #8 on promoting "inclusive and sustainable economic growth, full and productive employment and decent work for all" strives to "Achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive

sectors."[27] The internet has been called the "great transformer" and is viewed by many in all corners of the globe as a great enabler of economic growth and prosperity. According to one study by McKinsey, the internet "contributed 7 percent of [GDP] growth over the past 15 years and 11 percent over the past five." [28] The same study found that "Internet ecosystem maturity related to rising living standards," and that "the internet drives business transformation and economic modernization."[29] However, a June 2014 study from the Center for Strategic and International Studies suggests that cybercrime results in a loss of .2 percent of GDP.[30]In order to foster consumption and encourage businesses to leverage the internet and other communications technologies, stakeholders must trust the systems they are using. Good cybersecurity supports economic growth by preserving the trust in and therefore the benefits of digitization and IT systems.

Sustainable Development Goal #10 strives to "reduce inequality within and among countries."[31] As much as technology could reduce economic inequality and enhance trade, bad cybersecurity can exacerbate existing inequalities. Cyberattacks affecting digital commerce, critical sectors, and government agencies threaten to undo advantages gained through digitization. As the IGF cybersecurity report notes,

> Effective cybersecurity is essential 'to engage fully in the increasingly cyber-dependent [sic] trade and commerce. Robust cybersecurity frameworks enable individuals, companies and nations to realise the full potentials of the cyberspace, without fear or reservation, promoting cross-border delivery of services and free flow of labour in a multilateral trading system.'[32]

Because evidence of cyber insecurity leads to mistrust in the ICT environment of a country, cyber insecurity puts lower-income countries at a disadvantage on trade and foreign investment. How, for example, can lower-income countries competitively offer services and platforms in the global market if they are deemed insecure? How can developing countries attract foreign direct investment if the ICT environments are perceived as risky? The gap between cybersecurity haves and have-nots could create further obstacles to more evenly distribute the benefits of digital inclusion.

Finally, on the economic front, Sustainable Development Goal #9 seeks to "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation," because efficient infrastructure generates employment and wealth and can drive economic growth.[33] These infrastructures include ICT infrastructure, but also things like transportation and manufacturing infrastructure. Although not specifically in the lower- or middle-income context, the 2017 outbreak of the WannaCry ransomware attack clearly demonstrated the

capacity of actors to disrupt digitized sectors, disrupting transportation systems, ports, and many others.[34]

Governance

The internet has the potential to be used for both good and ill. If it is insecure and used for ill, it could undermine good governance. Sustainable Development Goal #16 aims to "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels."[35] Nascent technologies and techniques—like digital hashing, blockchain, and cloud computing—hold great potential for reducing corruption and creating accountability structures for public institutions. Relatedly, SDG #11 strives to "Make cities and human settlements inclusive, safe, resilient and sustainable."[36] The rise of electronic governance (e-governance) and government (e-government) as well as the potential for big data to drive better policy decision-making has led to greater efficiency in the delivery of services, tallying votes, collecting and utilizing information on the citizenry to craft better policies, and more.

The potential of ICT to help achieve these goals is unquestioned. However, as with economic growth, strengthened governance institutions and services based on technological interventions must be underpinned by trust in those technologies. India's experiment with biometric and digital identification provides a clear case study in the potential for bad security to undermine the delivery of good governance and government services. Because so much personal data is stored in one place, the digital ID data set has become a frequent target for identity thieves and other criminals.[37] The result is that a project intended to enhance India's ability to govern may result in more and new problems for the same people whose lives it intended to improve.

Human security

Security, including cybersecurity, has traditionally been the purview of foreign offices and ministries of defense. However, cybersecurity is as much about human security as any other kind of security. A myriad of SDGs seek to address human security concerns. From ensuring the delivery of better healthcare (SDG #3) and ending hunger (SDG #2) to the delivery of critical utilities like water, sanitation, and energy (SDGs #6 and #7), ICT and digitization can deliver improved human security. Digitization in sectors like healthcare, agriculture supply chains, power delivery, and water and sanitation is yielding immediate dividends and improving the lives of millions around the world. However, as technology enables these improvements to reach more and more people, those same people become increasingly dependent on their reliable delivery. And yet, it is becoming increasingly easy to disrupt services like these via cyber means. In

digitizing these services, decision makers are creating new dependencies, which, if disrupted, could lead to not only net-zero outcomes, but potentially net negative outcomes.

As alluded to above, no sector was immune to the WannaCry ransomware and the healthcare sector in the United Kingdom was very publicly disrupted.[38] In addition, the world has witnessed at least two instances where cyber vulnerabilities were exploited to cut off power to entire regions during cold winter months.[39]

More people will be coming online, and they will be doing different things with it and coming from different perspectives and backgrounds, we need to ensure that the internet and connected technologies continue to provide the value it has provided to date. Put simply, as the network expands we need to do more to ensure it is secure.

These three pillars demonstrate that there is not only a good argument for greater attention to cybersecurity from those who work in development, but an imperative. Cybersecurity is not just about state on state cyberwar, it is about the economy, good governance, and human security.

Chapter 2: Mainstreaming Cybersecurity

Lower- and middle-income countries are not immune to cyber risk. Take, for example, one of the most high profile data breaches in the last five years, the Bangladesh Bank heist. Sometime between February 4th and 5th, a suspected nation-state, advanced persistent threat actor (APT) used Bangladesh Bank's networks and credentials to request upwards of US$851 million from various other financial institutions.[40] Bangladesh is not the only lower- or middle-income country to fall prey to a cyber attack in recent years. Indeed, Ecuador, the Philippines, and Vietnam all experienced similar incidents with their banking sectors. The novel risks are not confined to the financial sector, however. This exposure is evidenced by the targeting of the Ukrainian power grid successively in December 2015[41] and December 2016[42] as well as the spate of ransomware attacks that disrupted government services around the world, most notably in India.[43]

One trait that all of these countries have in common is that development donors and global financial institutions assisted in spreading internet use and bringing key sectors of their economies and government services online. Throughout this process of building better access and digitizing society, more could have been done to help these countries manage heightened and novel risks posed by increased use of information and communications technology, and development institutions should play a key role in building this cybersecurity capacity. In an era where APTs present challenges to defenders even in higher-income and more

cybersecurity-advanced parts of the world, middle- and lower-income countries are no less at risk.

In his seminal 1957 piece, "Technical Change and the Aggregate Production Function", Massachusetts Institute of Technology economist Robert Solow proved that technical change correlates strongly with increased production. Over the course of the next few years, technology came to be seen as the driver that international development could rely on to grow lower-income economies and pull countries out of poverty. Today, this mentality persists, and since the early 1990s, the prevailing technological driver has been information and communication technology (ICT). But the use of ICT for development (ICT4D) creates new risks that have, until recently, gone understudied, misunderstood, and unarticulated. As these risks and the measures needed to manage them clarify, so too does the imperative of folding these measures into development practice underpinned by ICT.

Indeed, among the nine principles contained in the globally recognized guidelines for international development practitioners, "Principles for Digital Development," addressing privacy and security is a top concern.[44] Since 2010, and as ICTs increasingly drive development outcomes, the need for more and better cybersecurity capacity building has only grown as nearly all pillars of society—from the economy to governance to social interaction—are or can be touched by ICT. Global trends only project this phenomenon accelerating, and projections suggest that nearly all sectors will be fundamentally affected, if not transformed, by new technologies in the next 20 years. These trends—increasing digitization of key industries and services, more and more internet users, and the rise of increasingly numerous and sophisticated cyber threats—signal that it is time to pay more attention to managing the risks of digitization in the developing world. In short, the time has come to fold cybersecurity in international development.

Thus, the call to build better cybersecurity capacity is not new. As early as 2010, the United Nations Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security recognized the importance of building the cybersecurity capacity of nations around the world and particularly in lower-income countries.[45] However, while digital development certainly exists, the work of the cybersecurity community exists largely separately from that of the development community. The goal of this report is to provide a roadmap for bringing these two communities (which we outline in greater detail later in this report) closer together to enable both to achieve their goals in a resilient and sustainable manner. This requires mainstreaming cybersecurity in development.

What does mainstreaming mean?

Despite recognition from the World Bank in 2016, except for a few select cases, cybersecurity has hardly been incorporated in development. Thus, the question remains: how exactly should cybersecurity be folded into international development? In the past, the development community has incorporated or focused on emerging issues as they percolated to the surface in one of two ways: prioritization or mainstreaming.

Prioritization is about identifying a key issue for the breadth of the development community to focus on. Prominent examples of prioritization from the last decade include the goals outlined in the Millennium Development Goals (MDGs) [46] or Sustainable Development Goals (SDGs),[47] like achieving universal primary education, reducing child mortality, or conserving the oceans. Priorities are often identified by leading development institutions, like the World Bank, and communicated to the broader community through strategy documents like the MDGs or SDGs. In most past cases, prioritization takes an existing development focus and elevates it for critical attention.

Mainstreaming seeks to fold a new issue into existing development practice as a new equity or consideration in the practice of the community. In contrast to prioritization, mainstreaming is most relevant in the context of an emerging issue that has the potential to cut across many or all areas of development or presents a novel risk to progress in development but may not yet receive requisite focus from the community. Perhaps the most notable examples of mainstreaming have occurred in the past two decades in the form of women's rights and human rights. Women's rights and human rights were mainstreamed in part because of the nearly universal recognition that these fundamental rights are instrumental to creating the type of world that we want and agreed to with the UN Charter. While cybersecurity may lack some of the intrinsic qualities of these two rights movements, it is nonetheless foundational. ICT and digital technologies pervade society and provide the opportunity to improve the state of fundamental rights. But if they are left insecure, they stand to threaten progress on securing not only these rights, but also the future of the economy and good governance. Although undoubtedly different in character, mainstreaming cybersecurity in development could draw lessons from these processes.

Cybersecurity in development faces a similar challenge to that of early ICT4D efforts in the form of limited resources and competing equities. To some, "using limited development assistance funds to finance ICT4D projects" is a misuse of resources "when in some countries, clean water and sanitation, and electricity seemed more pressing" for the local people.[48] While this argument misses the point that ICT could enable more efficient delivery of other development outcomes and has become somewhat antiquated, it is nonetheless emblematic of a broader challenge. A paucity of data and good metrics to support the importance of cybersecurity—and ICTs more broadly—to development is an important element behind this skepticism.

For all its positives, the development community is still plagued with challenges and cannot be seen as a monolith. Indeed, one of the most vexing challenges facing the development community is the rampant siloing of issues. This stove-piping manifests in the ways development organizations—from bilateral and multilateral aid agencies to on-the-ground organizations—organize. The World Bank, for example, is divided into 13 separate "groups", each of which take lead for a given pillar of development or sector of society. Introducing cybersecurity as a new issue or priority would likely spawn a cybersecurity stovepipe, when the reality is that it should cut across existing issues and priorities.

Later in this report, we build a framework and recommendations to begin mainstreaming cybersecurity across all development practice.

→ BOX 2

Lessons from Another Field: Mainstreaming Human Rights in Development

Human rights and cybersecurity are undeniably different fields. Although it lacks some of the intrinsic and visceral aspects that human rights possess as an issue, mainstreaming cybersecurity can draw an important lesson from the experience of mainstreaming human rights in development.

The mainstreaming of human rights in development was the result of a concerted effort on the part of the human rights movement to "operationalize the relevance of human rights to various fields of development."[49] The breakthrough was precipitated by two important shifts in approach.

The first was a shift of emphasis from the "right-holder" approach—expanding human rights opportunities for individuals—to the "duty-bearer" approach—ensuring that states and non-state actors understand, respect, protect, and fulfill human rights obligations. This introduces a large and long-standing challenge for the ICT industry, which is unlikely to reach a resolution in the near term.

The second was a shift from a violations approach—where the emphasis was on identifying and punishing human rights violators—to a policy approach, which "demands developing new tools to bring human rights concerns into forward-looking policy-making processes," like Human Rights Impact Assessments (HRIAs).[50]

In fact, the creation and implementation of HRIAs was the most obvious manifestation of the mainstreaming of human rights. In 2005, UN Secretary General Kofi Annan appointed noted international relations scholar and the force behind the MDGs, John Ruggie, the Special Representative on the issue of human rights, transnational corporations, and other business enterprises. Ruggie's mandate included "identifying and clarifying standards of corporate responsibility and accountability with regard to human rights."[51] In development, human rights impact assessments require six essential elements:

- A normative human rights framework,
- Public participation,
- Equality and non-discrimination,
- Transparency and access to information,
- Accountability mechanisms, and
- Inter-sectoral approach.[52]

A good template for measuring the digital risk impact of development projects and programs does not exist right now, but such assessments for corporations, lending institutions, and other development actors—underpinned by similar essential elements as HRIAs—could be an important tool to drive forward the conversation about the impact of cybersecurity on development outcomes. Cybersecurity risk management, and frameworks to enable it, has become a standard practice in many private and government sectors. These frameworks could be adapted and transferred into the development community.

A digital risk impact assessment would differ from existing frameworks and models insofar as rather than measuring the cybersecurity capacity of a recipient country, a digital risk impact assessment would provide a framework for identifying what risks the use of ICT for a development project exacerbate as well as novel risks posed by digitization in that particular project.

Part II: Understanding the Important Communities

Mainstreaming will be a challenge. In order to make progress, we need to understand two primary stakeholders: The development community and the cybersecurity capacity building community. These communities, and the benefits of bridging them, are described here.

Chapter 3: Understanding Development

Two distinct communities of practice hold equity in mainstreaming cybersecurity in development. The first, the international development community, has existed as a community of practice for the better part of a century. The second, the cybersecurity capacity building community (which we cover in more detail in Chapter 4: Understanding Cybersecurity Capacity Building), has existed for closer to a decade and developed largely outside of major development institutions. These two communities possess complementary and often overlapping goals, yet in large part they operate in isolation from one another. To successfully mainstream cybersecurity in development, the work and lessons from the cybersecurity capacity building community must be folded into the development community. Understanding the activities, organization, and equities of each will be key to bringing these two communities together.

In this section, we provide a high-level overview of what constitutes the development community, how it works and is funded, what it does, and its notable equities when it comes to cybersecurity. If you are already deeply familiar with the inner workings of the development community, skip this chapter and move on to Chapter 4: Understanding Cybersecurity Capacity Building.

Organization

The development community can be divided, in large part, into four categories: (1) institutional donors, (2) bilateral aid agencies, (3) intergovernmental organizations, and (4) nongovernmental organizations.

Figure 1: The Development Community[53]

Category	Examples	Potential Activities
Institutional Donors	The World Bank, African Development Bank, Inter-American Development Bank, the International Monetary Fund	Provide expertise and funding, develop strategies
Bilateral Aid Agencies	U.S. Agency for International Development, DFID, Norwegian Agency for Development Cooperation (NORAD), Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), European Union	Provide expertise and funding, develop national strategies
Intergovernmental Organizations	The United Nations Development Program (UNDP), The Organisation for Economic Co-operation and Development (OECD), Organization of American States (OAS), Economic Community of West African States (ECOWAS)	Provide expertise and funding, assist with strategy development and implementation
Nongovernmental Organizations	Oxfam, The Bill and Melinda Gates Foundation, Doctors Without Borders (MSF)	Provide expertise and funding, assist with implementation, advocate

---

→ BOX 3

Featured Case Study: How Does the World Bank Work, Exactly?

The World Bank Group is a "global partnership [of] five institutions working for sustainable solutions that reduce poverty and build shared prosperity in developing countries," and is one of the most prominent members of the development donor community.[54] The bank's five institutions—IBRD,[55] IDA,[56] IFC,[57] MIGA,[58] and ICSID[59]—have "their own country membership, governing boards, and articles of agreement," but nonetheless work together with both the public and private sectors to connect "global financial resources,

knowledge, and innovative solutions to the needs of developing countries."[60] IBRD provides "financial development and policy financing," IDA provides "zero- to low-interest loans and grants," IFC "mobilizes private sector investment," MIGA "provides political risk insurance," and ICSID settles disputes.[61]

The World Bank has 13 sector-based global practices, which work with regional units to develop and fund projects and programs. For projects in lower-income and conflict countries, the IDA portion of the bank leverages grants and credits (zero- or low-interest loans). For projects in "middle-income and creditworthy low-income countries," the IBRD provides "loans, guarantees, risk management products, and advisory services."[62] Because loans require a counterpart in the recipient government who is willing to borrow (and therefore repay), loan financing is largely demand-driven.

In every case the World Bank works with a client or recipient country to develop a project or program based on the client's specific needs. The bank uses tools, like maturity assessments, study tours, and cybersecurity strategies, to help clients understand cybersecurity risk, but the use of World Bank resources is largely driven by the recipient countries themselves.

In addition to the work of IDA and the IBRD, the bank leverages trust funds through the Development Finance Vice Presidency (DFi).[63] These trust funds are often used to develop knowledge, support pre-implementation work, and pilot new models. They comprise the pot of money the bank relies on to explore new areas for investment. The investment from trust funds is roughly equal to all other lending done by the bank. Importantly, these trusts are funded via bilateral development institutions and the private sector. Some broad conditions for donations to trust funds—like the stipulation that a given donation must be spent on cybersecurity projects—can be negotiated by donors to the funds, though some restrictions on conditions exist.[64]

Finally, the bank's institutions can leverage Reimbursable Advisory Services (RAS)—an instrument to deliver specific "technical advice, analytical services, and implementation support" to eligible clients requiring services that cannot be fully funded from the bank's country program—for middle- and high-income countries.[65] The World Bank is "then reimbursed for the costs of delivering these advisory services," by the recipient. This portion of the bank's work, however, is comparatively small.

Once a lending project or program is initiated, the recipient government is generally responsible for "executing" the project and the recipient, using funds provided by the bank, generally enters into contracts with the private sector to implement the project. Large consulting companies that are able to manage the risk of bidding for projects in low-income countries dominate implementation of many ICT-driven projects. The World Bank and other donor

institutions have some measures, like debarment (also known as "blacklisting"), for private entities that abuse World Bank funds.

The way major institutions organize themselves can be seen as a legacy of early ICT for development phases from the 1990s and early 2000s. The early infusion of digital technologies into development practice with a focus on connectivity meant that many of the "digital development" practitioners were folded into existing transportation development teams, due to the similarities in "connecting" people. This structure is maintained today within the World Bank's Transport & ICT Global Practice. Though the World Bank was a leader in folding an ICT practice into their work, other major development organizations have created separate teams focusing on digitization. In the case of the World Bank, these sector-specific teams or groups then often work closely with country-specific teams to craft projects or programs tailored to specific aid and project recipients in the form of Country Partnership Frameworks (CPFs) and Systematic Country Diagnostics (SCDs) which identify core local challenges and guide the bank's support to a given country.

As digital technologies became increasingly important across sectors, the stovepipes in many of the prominent development organizations became more rigid and impermeable. In most cases, rather than enabling digitization specialists who could assist with digitization projects across different sectors, folding digitization into existing portfolios became the task of existing teams. In practice, for example, this meant that financial sector specialists led the digitization efforts for banking systems. The primary exception to this rule was, again, the transport groups in most major development organizations. Rather than focusing on digitization of specific sectors, transport became the home for connectivity initiatives focused on increasing the percentage of a given population able to access the internet.

In recent years, as major development institutions have begun to view "digital, data and technology as enablers rather than an end goal," some have begun to reorganize to better reflect this reality, sprinkling "digital" throughout their programmatic areas, rather than creating a new digital stovepipe. However, progress in many of the larger institutions is slower.

Relevant activities

Two separate strands of development activity—which are sometimes conflated—are pertinent to cybersecurity capacity builders: connectivity initiatives and digitization programs.

Connectivity initiatives seek to build out internet infrastructure in order make the internet reach more of the population. These initiatives often also focus on providing the broader population of a country or region with the tools necessary to leverage newfound connectivity, like computer literacy. Running fiber optic cables to rural areas or increasing 4G satellite coverage and distributing cellphones are examples of connectivity initiatives.

Digitization efforts, by contrast, focus on bringing technological advances—like computer systems, networks, and the internet—into different aspects of society to improve efficiency. Often associated with the concept of "going paperless," bringing government services online and the advent of e-banking are examples of digitization. Digitization can be digitizing existing industries, processes, and infrastructure, but can also involve just about any other project that incorporates or creates reliance on ICT. Connectivity and digitization are complementary. The more connected a given country, the broader and greater the impact digitizing key industries or services.

Funding

The way development donors support these activities varies depending on institution. The way multilateral donor institutions like the World Bank and the regional development banks raise their funds is complicated, but includes things like "funds raised in the financial markets, from earnings on its investments, from fees paid in by member countries, from contributions made by members (particularly the wealthier ones), and from borrowing countries themselves when they pay back their loans."[66]

At the World Bank, the International Development Association (IDA), the institution that gives no-interest loans and grants, is the primary recipient of contributions from donor countries, though it has recently incorporated other funding mechanisms into its work.[67] Country contributors can put conditions on their contribution and donors may attempt to steer money to a "limited number of 'special themes'" during the process of replenishing IDA's reserves, which happens every three years.[68] Once money is allocated, the bank's 13 global thematic teams and regional units then work with recipient countries to develop projects funded by this money.

Most major multilateral development finance institutions also utilize trust funds to support conceptual or pre-implementation work, pilot new models, and develop new knowledge. Thus, donor institutions often rely on trust funds to expand their work into new areas. In the World Bank's case, these trust funds provide "predictable multi-year funding that is crucial for effective development," and allow donors to "coordinate and target their scarce aid

resources across multiple sectors."[69] The trust money is often used alongside other "projects developed and financed" by the lending institution.

The funding structures of bilateral aid agencies, like DFID and USAID, are relatively simple in comparison to their multilateral brethren. Although there is some variation in how funds are appropriated, these agencies are generally funded by national governments via taxpayers. In most cases, an aid agency is tasked with developing a budget request, which outlines the strategy for spending its allocation to be approved by national governments or boards. In some cases these bilateral aid agencies will allocate funds to global donor institutions in the form of trust funds, as discussed above.

Notable equities

The primary objective of the development community is to reduce inequality and cultivate better opportunities and outcomes for all people. The community coalesces around the SDGs. However, how the community has gone about achieving its goals has morphed over its many decades of existence. Today, a key equity worth understanding is the development community's relationship with metrics.

Rooted in the economics discipline from its beginning, the development community, and donor institutions more specifically, rely heavily on metrics to decide how to spend money and monitor and evaluate their projects and programs. For prominent development economist Joseph Stiglitz, good metrics are imperative for development because they, "monitor and diagnose what is going on," provide a means to "assess the source of the changes," and "motivate civic action."[70] In many cases, these empirics are quantitative, though recent push back against Gross Domestic Product (GDP) as a primary measurement has lent a resurgence to qualitative metrics. However, because "society is too complicated to be summarized in a single number," Stiglitz and other economists have advocated for the use of a dashboard "small enough to be easily digested [and] large enough to include monitors of key issues."[71] Rubrics for evaluating development practice do not conflict with the aims of cybersecurity capacity builders, and lessons from the development community's experience in developing these rubrics can provide pathways for progress in the cybersecurity capacity building context.

→ BOX 4

Metrics and Development Economics

As early as the 1930s, economists—the early acolytes of development practice—recognized the importance of measuring economic growth. As Simon Kuznets posits in his 1934 piece, "there is considerable value… in checking the unarmed observation of even a careful student by the light of a quantitative picture of our economy."[72] Joseph Stiglitz, one of the fathers of modern development economics, further insists that "metrics are important not just because they tell us how we are doing but because they serve as guides in policy-making."[73] For decades, measuring development outcomes often relied on aggregate metrics like gross domestic product (GDP) or gross national product (GNP). However, economists have long noted the shortcoming of some these kinds of aggregate metrics.

In a 1934 report to the U.S. Congress, Kuznets notes that, "the welfare of a nation can scarcely be inferred from a measurement of national income."[74] Kuznets further expounds that "the national income total is… an amalgam of relatively accurate and only approximate estimates." Because of this flaw, "small differences or changes [in these metrics] should not be taken as unequivocal indications that differences actually exist or that changes have actually occurred."[75]

In recent decades, and in part due to interventions from the likes of Stiglitz, development institutions have stressed the importance of more detailed metrics to monitor and evaluate the efficacy of development interventions on different outcomes and overcome "GDP fetishism."[76] This ethos permeates the development community to the extent that one development scholar likened it to a "fetish" and urges the cybersecurity community to proceed cautiously so as to not fall prey to some of the same pitfalls that over-reliance on metrics caused in the development community.[77]

Chapter 4: Understanding Cybersecurity Capacity Building

At a high level, there are two primary goals of the cybersecurity capacity building community—develop cybersecurity capacity around the world to (1) safeguard against systemic ICT risk (i.e. risk to the global financial system), and (2) deliver sustainable dividends from digitization and increased ICT adoption. Although more empirical work is needed to draw correlations, the work of the cybersecurity capacity building community often contributes directly to the achievement of SDGs and sustainable human progress more broadly, as described in Chapter 2. Most of the SDGs and the targets that contribute to them imply the use of ICT to further human development. In many of these cases,

cybersecurity—and by extension the work of the cybersecurity capacity building community—serves to underpin confidence and trust in these ICT systems.

Organization

Today, the cybersecurity capacity building community consists of a set of broad categories of actors not dissimilar to those of the development community. The nascency of this community of practice means that major actors and their roles are less clearly defined than in the development community. Although the primary actors are arguably technology companies and government agencies, intergovernmental and nongovernmental organizations play important roles as well. As Norwegian scholar Lilly Pijnenburg Muller noted in 2015, the composition of the cybersecurity capacity building community faces challenges of its own as a great number of organizations exist to help measure capacity and maturity, but actual capacity developers are less numerous.[78] Although the infusion of more money and the increasing maturity of the field have spawned more implementers, this problem persists today. In addition, the focus of some donor countries has shifted towards a model of exporting their experiences and frameworks as a part of their global cybersecurity agenda.

Figure 2: The Cybersecurity Capacity Building Community[79]

Category	Examples	Potential Activities
Government Agencies	UK FCO; U.S. Departments of State, Homeland Security, Justice, and Defense; German Federal Foreign Office; National Internet Development Agency of Korea (KISA); the Cyber Security Agency (CSA) of Singapore	Methodological support, technical support, infrastructure support, budgetary support
Technology Companies	Microsoft, Symantec, AT&T, Cisco, Huawei	Methodological support, technical support, infrastructure support

Category	Examples	Potential Activities
Intergovernmental Organizations	Organization of American States (OAS), Organization for Security and Co-operation in Europe (OSCE), United Nations Office on Drugs and Crime (UNODC), International Telecommunications Union (ITU), European Union (EU), The World Bank, Association of Southeast Asian Nations (ASEAN), Interpol	Methodological support, budgetary support, technical support, infrastructure support
Nongovernmental Organizations	Packet Clearing House, Oxford Global Cyber Security Capacity Centre, CyberGreen, Forum of Incident Response and Security Teams (FIRST), DiploFoundation, Internet Society	Methodological support, technical support, infrastructure support
Other Organizations	Global Forum on Cyber Expertise, The Hewlett Foundation, academic institutions	Methodological support, Budgetary Support

In part because there is no clear delineation of who is in and who is out of the community and in part because some of the budgets of capacity builders are not publicly available, it is next to impossible to identify a monetary amount spent on cybersecurity capacity building annually. However, the GFCE is in the process of consulting with its members to begin to grasp the scope of spending. Initial findings have not identified an authoritative amount spent on capacity building globally, but initial estimates suggest that the range of annual spending per "actor" ranges from US$8,000 to US$6,000,000.[80] Estimates for total public and private annual spending on cybersecurity capacity building globally based on interviews for this report range from roughly US$50 million to roughly US$1 billion, with the mean estimate far closer to the lower end of that spectrum.[81] Regardless, the scope of spending on this development challenge pales in comparison to spending on other issues, despite its cross cutting nature. By comparison, the total "sum of official development assistance, other official flows and private flows" from the OECD's Development Assistance Committee (DAC) countries alone totaled over US$315 billion in 2016.[82]

Because the community of practice is still immature relative to the development community, parts of the field still need to be built. Specifically, the cybersecurity

capacity building community has three shortcomings that could in part be aided by bringing the cybersecurity capacity builders closer to the development community.

First, as depicted by Figure 2, there is a great deal of overlap with regard to the potential activities and roles of different cybersecurity capacity builders. This overlap manifests not only in principle, but also in practice. Although one of the intended roles of the Global Forum on Cyber Expertise is to coordinate capacity building activity, its limited budget and secretarial capacity means that it is not fully delivering on this promise. In addition, information sharing between cybersecurity capacity builders could be improved. Too often, project information is shared bilaterally and after the fact. The cybersecurity capacity building community could do a better job of talking to one another before projects are funded and implemented.

Second, the methodologies for building cybersecurity capacity are underdeveloped. For development, major development economists and other social scientists helped drive forward methods and good practices in development. Due in part to the nascency of the issues facing cybersecurity capacity development, the academic community has not yet applied the same empirical rigor to identifying good practices for cybersecurity capacity building as it has in the past to understanding how to grow economies or develop good governance.

Third, there is a distinct shortage of implementers and on-the-ground, local networks. In many cases, cybersecurity capacity builders—donor government representatives, their contractors, corporations, and sometimes nonprofits—fly in, conduct a workshop or training session, and leave. While this is not universally the case and some projects or programs involve more extended in-country engagement, these projects appear to be the exception rather than the rule. This reality is driven at least in part by the lack of local, grassroots networks, but is also a reflection of the relative global scarcity of the expertise and funding required to build cybersecurity capacity.

Activities

Klimburg and Zylberberg provide a useful typology for describing cybersecurity capacity building activities of donor countries, outlined in Figure 3.[83] Each of these categories of activity generally aim to improve the cybersecurity posture of recipients as a means to enable greater dividends from digitization and increased ICT access.

Figure 3: Activities of Cybersecurity Capacity Builders[84]

Support Type	Description	Examples
Methodological	Delivering models and "policy options available to governments considering" cybersecurity capacity building activities	Developing a national cybersecurity strategy Assisting in crafting cybersecurity regulation or legislation Providing methodological support for technical, infrastructural and budgetary activities
Technical	"Training around the CERT/CSIRT structures" as well as "the help provided at law-enforcement level and support for community-based instruments"	Joint cybersecurity exercises Sale of technical cybersecurity tools and training Cyber forensics training Cybersecurity educational programs
Infrastructural	Providing expert support for the secure provision and deployment of technical infrastructure	Assistance securely digitizing critical infrastructure Configuring firewalls and other security controls
Budgetary	Providing funding for direct, operational expenses as well as providing funds for large scale infrastructure development and "sustained local engagement with partner governments"	Funding the development of a national CSIRT Funding for workforce development programs Funding diplomatic participation in international cybersecurity conferences or meetings Funding for awareness campaigns

As depicted by Figure 3, the activities of cybersecurity capacity builders are diverse. Nonetheless, Oxford's Global Cyber Security Capacity Center (GCSCC) and the GFCE have built a portal that attempts to capture all the cybersecurity capacity building initiatives and activities.[86] Among the activities are things like "capacity building workshops for parliamentarians and senior civil servants,"

"practical awareness training and campaigns," crisis management exercises, and computer emergency response training material.[87]

Funding

Where development activities largely follow a structure where donors provide grants to recipients for programs and those recipients then execute specific projects (mostly) through a private sector implementer, cybersecurity capacity building does not follow the same model. Often, the donors, which are primarily foreign ministries from around the world, work directly with implementers which are sometimes private companies (like MITRE Corporation, which does much of the implementation work on behalf of the U.S. government), but can also be government agencies or competencies themselves. In many cases, rather than giving grants or loans directly to recipient countries, grants go directly to implementers earmarked for work in recipient countries. Separately, several private companies contribute resources to building better capacity on their own, without additional financial contributions from governments or other donors.

The work of the community is important, and the world's critical infrastructure and information systems would be far less secure without it. However, given anecdotal evidence from high-profile incidents like the global ransomware attacks, the breaches of the SWIFT system, and the continued increase of DDoS attacks, there can be little doubt that far more work needs to be done. The current scale of the community—both in terms of human capacity and financial capacity—is not sufficient.

Chapter 5: The Necessity of Bridging these Communities

These two communities, which have existed largely separately since cybersecurity capacity building became a community of practice around a decade ago, each contribute to the sustainability of development and should be placed in positions of complementarity and coordination rather than viewed as purveyors of separate and sometimes competing activities.

Some countries have piloted projects to bring development experts from their bilateral development institutions together with cybersecurity capacity builders from foreign ministries. The U.K., for example, has piloted projects that bring the development experts of the Department for International Development (DFID) together with the cybersecurity capacity builders in the Foreign & Commonwealth Office (FCO). The Dutch have engaged in a similar process. However, most countries lag far behind.

Learning opportunities

Despite the tepidness of the institutional response of most development organizations, the benefits of bringing these communities together to mainstream cybersecurity in development programs and projects are numerous. For a start, the development community possesses decades of expertise on capacity development, from which the cybersecurity capacity building community would benefit. Cybersecurity capacity building is not immune from some of the same plights that have plagued other development fields. For example, the development community has wrestled with identifying and measuring good practices for several decades. The Global Forum on Cyber Expertise is now working to identify global good practices in cybersecurity capacity development, but could draw valuable methodological lessons from past experiences in the development community.

Just as the cybersecurity community can bring extensive cybersecurity expertise to the development community, the development community can bring extensive experience and expertise in building capacity and capacity development and on-the-ground experience and networks. This could be crucial for improving the delivery of cybersecurity capacity building programs as many of the organizations that provide cybersecurity capacity building have little or no presence on the ground. This reality can sometimes jeopardize projects. Drawing on the development community's local presence and association with grassroots actors could be critical in enabling the delivery of better cybersecurity capacity building programs.

Avoiding a missed opportunity

Mainstreaming cybersecurity in development will also prevent the lower- and middle-income world from missing a key opportunity: learning from the mistakes made during digitization in the higher-income parts of the world. As prominent computer science pioneer Peter G. Neumann noted when reflecting on the insecurity of the modern internet, "The fundamental problem is that security is always difficult, and people always say, 'Oh, we can tackle it later,' or, 'We can add it on later.' But you can't add it on later. You can't add security to something that wasn't designed to be secure."[88] As Steve Corker, former chair of the board for the Internet Corporation for Assigned Names and Numbers, notes, "we could have done more [to build security into the internet from the beginning], and most of what we did was in response to issues as opposed to in anticipation of issues."[89]

Decades of experience in trying to secure digital systems in early adopting areas has led many cybersecurity professionals to wish that security had been given more credence in the early stages of digitization. The later adopters of digital technologies have an opportunity to learn from those mistakes. Bringing the cybersecurity capacity building community and its expertise into development

circles will enable the development community to institutionalize these learnings and leverage the cybersecurity community's expertise and networks.

Funding for better cybersecurity

Though not the primary goal of mainstreaming cybersecurity in development, an ancillary benefit of mainstreaming cybersecurity in development would be greater financial resources devoted to building cybersecurity capacity around the world.

It is difficult to pinpoint the exact amount spent by Ministries of Foreign Affairs, intergovernmental organizations, civil society, and industry on cybersecurity capacity building. However, every interviewee from both the cybersecurity capacity building community and those we spoke to in recipient countries cited a lack of funding and high costs as one of the primary barriers to developing cybersecurity capacity. Unlocking development assistance in its many guises to help build cybersecurity capacity is one of the many ancillary benefits of mainstreaming. This includes the likes of Official Development Assistance (ODA)—a term meaning money provided by official government agencies for the promotion of economic development and welfare of developing countries as its main objective[90]—as well as the work of donor institutions and private philanthropy more broadly.[91]

Part III: Challenges and Solutions

Mainstreaming cybersecurity in development will face major challenges. Here we outline what some of these challenges might be and offer a set of actions that could directly contribute to overcoming them.

Chapter 6: Major Challenges to Mainstreaming

This chapter describes the current set of barriers to better integrating cybersecurity into development projects and programs. As the international community wrestles with these challenges, it must consider several key stumbling blocks that can be identified and removed to clear the path to greater integration of cybersecurity in international development. Here we outline the nature of four prominent, identified challenges.

Challenge 1: Reticence from development donors

Donors—organizations and individuals that fund development projects—are a large and influential part of the broader development community. Donors come in all shapes and sizes, from entrepreneurs looking to break into emerging markets, private philanthropists, and philanthropic organizations to bilateral, government-run and government-funded aid agencies and massive development banks, like the World Bank. These donors wield influence through carrots, like the promise of more money as a reward for good practice, and sticks, like loan cancellations and loan conditions. While donors most often work with recipients of the investment or loan to tailor a project or program to fit the recipients' needs, donors do, nonetheless, have a great deal of agenda-setting and steering power. For this reason, generating greater understanding of the importance of cybersecurity to safeguard and enable the investments of the donor community is crucial. In this section, we will explore obstacles to doing so.

The first, and perhaps primary, challenge to mainstreaming cybersecurity in development revolves around the use of metrics to define and track success or failure in cybersecurity capacity building. The donor community's focus on metrics poses two specific challenges to the cybersecurity capacity building community.

First, the donor community's reliance on metrics to steer investment means that the cybersecurity capacity building community will need to create an empirically convincing argument that an absence of better cybersecurity leads to demonstrably worse outcomes. Second, in the event that the need to integrate cybersecurity into development is empirically convincing, the cybersecurity community more broadly has yet to develop truly useful measurements to

evaluate cybersecurity and cybersecurity capacity building interventions. Lacking these metrics, it becomes difficult to craft meaningful, empirically driven arguments for what capacity development interventions produce the most positive outcomes. Better outcome-oriented metrics are needed to identify and communicate these good practices, whether government policy interventions, corporate policies, or technological interventions. This is a challenge in cybersecurity, as the field is still in the process of developing reliable metrics and the environment changes rapidly with updates in technology. But as Sami Saydjari notes, "cybersecurity can be effectively measured using risk," and "good metrics predict risk," allowing engineers and others to mitigate it.[92]

As Pawlak notes, "there is no single good model for security in cyberspace."[93] This reality is acknowledged by the Digital Dividends report, which notes that, "In the areas of cybersecurity, there are few obvious policy recommendations, and in these areas—perhaps more than others—governments can play a role in developing effective policies."[94] This maturing process is one that the development community has experienced in other areas and is well placed to assist the cybersecurity capacity building community with the growing pains. For Pawlak, "the exchange of good (and bad) practices between individual countries and regional organizations may help streamline ongoing efforts."[95] While Pawlak is right, there is an additional opportunity for the cybersecurity capacity building community to take its cues from the development community in terms of both how good practices are spread and by mirroring the empirical rigor that goes into proving the efficacy of those practices. Dutton et al. suggest a number of metrics that may be usable for these purposes which could describe things like end-user security, cybersecurity capacity, its outcomes, and reliability.[96] The results of their study suggests that cybersecurity capacity building is a "worthwhile investment," but more work is still needed on this subject.[97] By better incorporating empirics in the day-to-day of cybersecurity capacity building, the practice will begin to better resemble the good practices of international development more broadly.

In addition to this metric challenge, Sandra Sargent, a cybersecurity expert at the World Bank, has outlined two prevailing myths that exist in the donor community that she suggests are major barriers to a higher degree of buy-in from leaders in this community.[98]

The first myth is that cybersecurity is all about security in the traditional military sense. Sargent suggests that instead, cybersecurity should be communicated as about the economy, governance, citizens, companies, banks, hospitals, lives, growth, and development. In order to dispel this myth in the development community, more work is needed to develop standardized and comparable data sets and robust analytical work showing the cost-benefit of investments into cybersecurity versus the costs of not investing.

The second myth is that the donor community is not well equipped to deal with the issue of cybersecurity. To Sargent, this is false because the donor community has cross-disciplinary expertise needed to address the pan-societal challenges posed by cyber risks. The donor community also has worldwide coverage, country presence, and in-depth knowledge of the local conditions needed to reach the most disadvantaged and least prepared to manage cyber risk. In addition, the donor community has the financial resources that can close gaps in cyber readiness if applied in a coordinated manner, and the use of international frameworks and agreements to bring greater collaboration and consensus. In order to dispel this myth in the donor community, there is a need for greater coordination of activities at a country level and a need for a standard set of tools and mechanisms for cybersecurity capacity building.

Communicating the benefit of cybersecurity is a challenge that plagues the cybersecurity community even outside the context of development. In the context of development, as the World Bank notes, "much of the benefit of the internet is unmeasured."[99] Compounding this shortcoming, the benefit of better cybersecurity is potentially unmeasurable, as greater cyber risk management results in an absence of activity, much of which is not actively blocked, but is instead never seen. The development donor community is slowly beginning to realize the risk posed by a lack of cybersecurity, which represents a risk to lending portfolios, a capacity building opportunity, and a crucial component of future progress, but a great deal of work is still required to communicate the need to community more broadly.

Challenge 2: Helping aid recipients spend wisely

At first blush, breaking through the reticence of recipients may seem less imperative than creating buy-in at the donor level. However, in modern times, the recipients of development assistance are (rightly) highly influential in identifying where and how to spend development dollars. While aid recipients are increasingly aware and interested in investing in cybersecurity, three primary challenges prevent them from doing so:

- The complexity and technological nature of cybersecurity and risk management sometimes leaves aid recipients unsure where to start,
- The perception that internet access and cybersecurity are competing for political attention and finances, and
- Cost.

The first challenge, overcoming the feeling on the part of recipient countries that cybersecurity is overwhelmingly technical and complex, is perhaps the most pressing challenge, but also the one potentially simplest to solve. In many lower-income parts of the world, the appetite for cybersecurity has grown

tremendously, but oftentimes it is unclear to these countries where to start.[100] Cybersecurity maturity models are a tool often used by capacity builders in an effort to help demystify cybersecurity and provide a guide for how to improve cybersecurity capacity maturity. These models are a step in the right direction, but lack certain elements that could be most useful to countries in dealing with limited budgets and in the earlier stages of cybersecurity capacity development. Current iterations of these models, like Oxford's *Cybersecurity Capacity Maturity Model*,[101] the Potomac Institute's *Cyber Readiness Index*,[102] and the Australian Security Policy Institute's *Cyber Maturity in the Asia-Pacific Region* report,[103] focus primarily on measuring the existing cybersecurity maturity or capability of a given country. They can then be used to help craft strategies and can be used to measure progress.

While useful, these models leave a gap in the market for information that has been requested from developing governments: an outline of what cybersecurity capacities to prioritize for development and when. This type of diagnostic framework could help countries not only understand their level of cybersecurity maturity, but also the broader local ICT context and where the best areas of strategic focus might be. Existing models often provide tiers for development, but they do not map to the ICT maturity of a given country. A complement to these existing models should focus on answering this question of what to prioritize and when. Such a framework should focus on providing a toolkit for the measurement of general ICT maturity across society—from economic to social to governance—matching these stages of maturity to and understanding of a country's threat landscape to identify core cybersecurity needs. For example, if a country has focused predominantly on creating greater access to the internet but has not taken steps to digitize their financial sector, they need not focus on building incident response capacity in their financial sector but should instead focus on raising public awareness and education.

A second major barrier lies in the narrative around ICT access versus security. For many in both development institutions and lower-income countries, a limited budget for ICT projects means access and security are often pitted against one another as competing interests for funding. This is true in a literal sense: it costs money to deploy new fiber optic infrastructure and it costs money to fund a CSIRT; the funding for these two types of activities comes from the same pot of money. However, increased access to and reliance on ICT for greater swaths of life without ensuring the trust and reliability of ICT is likely to yield suboptimal development outcomes. Furthermore, a country that demonstrates a commitment and plan for improving cybersecurity is likely to attract increased lending or grants for ICT connectivity. Factoring in cybersecurity will reduce the risk to lending that has ICT dependencies and increase the strength of a development impact case through increased trust, greater resilience, and reduced harm.

The third major barrier for project recipients is related to the last, and that is the cost of improving cybersecurity. Again, this challenge presents two layers. First, in part due to shortfalls in metrics and in part due to the nebulous notion of "improving cybersecurity," it is difficult to accurately and reliably cost out the price of doing so. Second, in an environment of very scarce economic resource—the circumstances in most lower-income countries—high cost for activities or investments that are unlikely to yield immediate, visceral impacts can be prohibitive. We discuss this particular challenge in more detail in Challenge 3.

→ BOX 5

Speaking the Language of Development

Although the language used in much of the development community and the cybersecurity capacity building community is the same, the presence of a great number of terms of art, particularly in the development community, can lead to breakdowns in understanding. Indeed, development discourse's "buzzwords and fuzzwords" have been the subject of an entire book.[104] As Cornwall and Eade note, language matters for development. Development terms are often passwords "to funding and influence" in the community, and development lingo is rife with "contested terms," just as the terms cybersecurity and information security are contested at the international level.[105] Fortunately, development and aid agencies around the world have developed glossaries of development terms, in an effort to minimize misunderstandings.[106]

One highly contested term in the development community is that of "security". In some parts of the world, like Latin America, the word security (seguridad or seguranca) is not universally positive. Indeed, in these and other parts of the world, security does not necessarily refer to the security of the citizens, but instead to the security of the state, which can actually threaten the security of individuals. In addition, apart from securitization concerns on the part of recipients, some in the development community view security as inherently political and development as necessarily apolitical, while tacitly acknowledging some politicization. Indeed, the term cybersecurity is an inherently political term globally. Information security, which encompasses broader security considerations, like the control of online content, is preferred by some parts of the world to cybersecurity, which describes a more narrow focus on computer and network security.

Nonetheless, while the term cybersecurity has likely reached a path-dependent point in discourse about managing cyber risk, changing the way that

cybersecurity is described could go a long way in changing the perception of securitization. At the end of the day, cybersecurity is about building trust in the technologies and managing new risks borne out of them.

Challenge 3: Balancing with other development equities

The challenge of balancing cybersecurity with other development equities is twofold. First, many issues under the development umbrella battle for attention. This phenomenon is perhaps illustrated best by the 17 different Sustainable Development Goals. Mainstreaming, rather than merely prioritizing cybersecurity in development will help manage this attention issue.

However, development funding is not bottomless and the presence of different offices, focuses, and equities even within individual donor institutions creates a highly competitive funding environment. Often, the activities of donor institutions are driven by the way these institutions raise their money for projects, as outlined above. Donor institutions—both bilateral and multilateral—must argue compellingly to raise their money. This reality means that issues that get the most development attention outside of these institutions—and are therefore most likely to obtain funding—receive the most budgetary attention. These other equities, which are largely summed up by the 17 SDGs, include things like ending poverty and delivering clean water to all. Policymakers seeking to mainstream cybersecurity in development must understand that, while cybersecurity often contributes to the attainment of development goals, it is not always that primary contributor and sometimes other equities will justly receive greater attention and funding.

Challenge 4: Building cybersecurity capacity in the development community

Integrating cybersecurity talent into the development community is necessary to equip the community with the expertise to implement cybersecurity capacity building projects on the ground and mainstream cybersecurity in their programs at a strategic level. Nonetheless, some in the development community are resigned to seeking external help via contracts. While the expertise needed certainly exists in law firms which can help with contract issues and consultancies that can help navigate complicated sub-project pitches, profit motive can lead to advice that encourages less efficient or effective spending.

As one development professional noted, "As a development group, we will never be the leads on cybersecurity. We rely on cybersecurity partnerships for actual implementation."[107] Whether or not major development agencies and donors

need to or could retain operational cybersecurity expertise is debatable. The benefits are numerous—in-house expertise is likely to be cheaper in the long run and can develop institutional knowledge and programmatic expertise—but the short-term cost of bringing expertise into these organizations and retaining it may be prohibitive. However, even if we are to accept that operational cybersecurity expertise will not and perhaps should not be housed in development organizations, there is little doubt that one major role of large donor institutions remains providing aid recipients "with the tools to make informed development decisions for lasting impact."[108] In order to continue playing this role in the digital age, donor institutions will necessarily require some kind of cybersecurity advisory capacity. This being the case, recruiting cybersecurity talent into the development community writ large poses two general challenges, which are worth highlighting here.

First, the cybersecurity industry has a talent shortage. The Center for Cyber Safety and Education estimates that the global cybersecurity workforce gap will reach 1.8 million workers by 2022.[109] Globally 66 percent of professionals believe that there are too few cybersecurity workers in their department.[110] Reasons for this shortage are numerous and include explanations like, "qualified personnel [are] difficult to find," "requirements [are] not understood by leadership," "business conditions can't support additional personnel," and "security workers are difficult to retain."[111] This labor shortage means that finding good workers in the private sector can be expensive. Indeed, the average salary of an information security worker in North America is US$120,000 per year.[112]

The second is an often-overlooked challenge: The vast majority of in-government cybersecurity expertise resides in somewhat opaque areas of government like law enforcement, intelligence, and the military. Juxtapose that opaqueness with the notion that development assistance rightly requires a great deal of transparency and the compounding effect of the labor shortage cited above. Because the development community generally avoids working with security partners from these communities, the provision of leading in-country government experts—should they exist—for development projects poses a challenge. However, in many countries, past military service members are an increasingly important and prominent part of the cybersecurity workforce and are a pool from which development organizations could acquire expertise.

With these general workforce challenges noted, it is also important to acknowledge that the skills needed in donor institutions differ slightly from the skills that most technical cybersecurity professionals possess. Whereas cybersecurity expertise needed to support programs and implementation is likely to mirror the conventional description of a cybersecurity worker—someone with a technical background and experience in a security operations center (SOC) or CSIRT—the skills needed to create informed customers are not necessarily operational security skills. Technical and policy nuance is needed, as is the capacity to weed out snake-oil solutions.

Chapter 7: The Way Forward

Understanding the compatible, complementary, and sometimes competing equities of the two communities is paramount for bridging the gap between them. However, a simple understanding is not enough to truly push the issue forward. Indeed, we recommend a two-pronged approach to mainstreaming cybersecurity in development. This approach will involve not only cultivating interest and buy-in from the donor and recipient communities, but in developing more tools to position the development community to succeed once high-level buy in is achieved.

For this reason, a strategy to mainstream cybersecurity in development can neither focus exclusively on strategic, top-down approaches (e.g. statements from heads of development agencies) nor only on operational, bottom-up approaches (e.g. building awareness and expertise in the operational development community). When orchestrating strategic shifts, one must always prepare the operational environment for success. We recommend the following actions:

1. ***Reframe cybersecurity in the context of development to focus on "security for" as well as risk management, resilience, sustainability, and trust.***
2. ***Build a library of credible and politically useful information on the impact of cybersecurity and cyber insecurity on development.***
3. ***Demystify cybersecurity for aid recipients.***
4. ***Bring more of the right cybersecurity expertise into donor institutions.***
5. ***Create and implement digital risk impact assessments for development projects and programs.***

A number of common themes are spread throughout the recommendations, of which one is the need to build an expert field. While field-building is critical, the field need not be built in a day, nor from scratch. Indeed, one of the keys to building the field will be to generate engagement from established authorities on development practice, many of whom reside in leading academic institutions. A key challenge that we hope to address gradually through these recommendations is this: Why haven't leading development economists—the Agarwals, Easterlys, and Stiglitzs of the world—gravitated to this topic and field?

These recommendations are designed to address five key considerations in an effort to make them as actionable and impactful as possible:

- What actions are needed to achieve this recommendation;
- What successful implementation looks like;
- How to make this happen, or at least some initial steps;
- Why this activity has not happened yet; and

- Who could lead these efforts.

While the recommendations are able to stand alone and progress in any of them would likely yield progress overall, they are complementary and progress on all of them is most likely to maximize progress on the whole. None of this is easy. If it was, it likely it would have already been done. While we acknowledge this is an uphill battle, we do our best to provide a detailed explanation of how interested actors, mostly in policy-making positions, might go about implementing these recommendations.

Recommendation #1: Reframe cybersecurity in the context of development

Cybersecurity, in the context of international development, has a narrative problem. According to one former development worker, the simple inclusion of the word "security" will likely scare some development parties away.[113] For another current development worker, the usual framing of cybersecurity as security from a given threat is unlikely to convince the development community of the importance of cybersecurity.[114] A refreshed approach to how the cybersecurity community discusses cybersecurity in the context of development to change the narrative around cybersecurity is a necessary step towards creating more buy-in at the top levels of the development community.

In 1998, noted international relations scholars Margaret Keck and Kathryn Sikkink conducted a deep analysis of historical issues that have been reframed and around which the discourse changed. Citing prominent examples like human rights in Latin America in the 1970s and 80s, the Anglo-American abolitionist movement in the middle of the nineteenth century, and others, the authors suggest that the most powerful way to change narratives is for "transnational advocacy networks" to create a "boomerang pattern" to influence states and international organizations.[115] A transnational advocacy network is a group of "relevant actors working internationally on an issue, who are bound together by shared values, a common discourse, and dense exchanges of information and services."[116] A boomerang pattern is essentially the process of building a broad network of advocates—from international institutions and states to NGOs and companies—to put pressure on an actor or community from different angles to change behavior.

For Keck and Sikkink, an effective boomerang pattern is created through the development of a coherent transnational advocacy network that deploys four main tactics (see Figure 4) in their efforts at persuasion, socialization, and pressure: information politics, symbolic politics, leverage politics, and accountability politics.[117]

Figure 4: The Four Political Tactics[118]

Tactic	Explanation
Information Politics	"The ability to quickly and credibly generate politically usable information and move it to where it will have the most impact."
Symbolic Politics	"The ability to call upon symbols, actions, or stories that make sense of a situation for an audience that is frequently far away."
Leverage Politics	"The ability to call upon powerful actors to affect a situation where weaker members of a network are unlikely to have influence."
Accountability Politics	"The effort to hold powerful actors to their previously stated policies or principles."

In order to successfully reframe cybersecurity and change this discourse around the issue in the development sphere, interested parties—like cybersecurity policymakers in foreign affairs ministries, the corporate sector, and nonprofits—must identify or create a transnational activist network and develop the capacity to leverage the four political tactics.

Here we outline two ways in which the cybersecurity capacity building transnational activist network must align their framing. In subsequent recommendations, we provide guidelines for how to develop the capacity to leverage information politics and symbolic politics (Recommendation #2) and how these recommendations would lead to the ability to employ leverage and accountability politics.

Operationalizing Recommendation #1

Actions:

- Shift the narrative to "security for" instead of "security from;"
- Reframe cybersecurity in the developing context around risk management, sustainability, resilience, and trust;
- Provide more opportunities for the cybersecurity and development communities talk to one another.

What does success look like?

The cybersecurity community adopting these framings in their engagement with the development community so that the development community adopts them as well.

Why is this feasible?

Because reframings of this nature have successfully taken place in other fields, though they take place due to concerted efforts and take time

How do we make this happen?

Leadership from key national governments; recruitment of private sector actors; funding and support for key nonprofits and academic institutions.

Why hasn't it happened yet?

This has only recently emerged as an international priority and there has been a lack of leadership and coordination of the transnational advocacy network. There are also constituencies, like the defense sector, that have an interest in talking about and framing the issue in other ways

Who could lead these efforts?

Civil society.

Action 1.1: Shift the discourse to "security for" not "security from"

The first narrative to align involves changing the framing of cybersecurity as "security from" to "security for" in the context of international development. For parts of the development community, when they hear cybersecurity, they think of building military capacity and cybersecurity as a means to combat threats *from* mysterious intelligence agencies, militaries, or non-state criminal cartels. While good cybersecurity practice certainly does try to insulate against these threats, the reductive rather than constructive framing does not correlate well to the sensibilities of the development community. Instead, a constructive framing of cybersecurity as an enabler *for* certain development outcomes will engender greater interest on the development side.

Cybersecurity and development are not alternatives and they cannot be sequenced. Cybersecurity enables development and development is what rationalizes security. Patryk Pawlak and others have done excellent work drawing out the impact of cyber insecurity on human development and human rights.[119] In the development context, cybersecurity is for consumer protection, for financial sector stability, for the reliable delivery of e-government services, and

for safeguarding privacy and basic human rights. It is crucial that cybersecurity leaders in government, civil society, academia, and industry begin to talk this way in their engagement with the development community.

Action 1.2: Reframe cybersecurity around risk management, resilience, sustainability, and trust

As Klimburg and Zylberberg noted in 2015, "the idea of connecting the term 'cyber security' with the term 'development'... is contentious."[120] This holds as true in 2018 as it did in 2015 and necessitates a second major narrative shift that must take place involving the framing of cybersecurity itself. When members of the general public hear the word cybersecurity the implicit notion is that society, an organization, or an individual could eventually attain complete cybersecurity and the end goal of "cybersecurity" is to become "cybersecure." As Microsoft cybersecurity researcher Troy Hunt notes:

> Security is not a boolean proposition. It's not "secure" versus "insecure," "safe" versus "unsafe." rather it is a spectrum of controls that all contribute to an overall security posture. There is no "fully", there is no "completely"; every system—every single one—has weak points and a sufficiently well-equipped and determined adversary will find them.[121]

It is the nature of software that vulnerabilities exist. It is the nature of the humans who rely on these technologies that we will not always create the best passwords or adhere to the good practices.

These realities mean that there will always be risk to using ICT. When risk will always be present, a better framing than "security" is "risk management" or "resilience." This framing is sensible because it is both the way that corporations and large organizations have begun to frame cybersecurity, and because these terms, risk management and resilience, are common and normalized in the development community.

Action 1.3: Provide greater opportunities for the cybersecurity and development communities talk to one another

Crucial to mainstreaming cybersecurity in development is physically bringing the two communities together more often to coordinate, share experience, and cross-pollinate ideas. In doing so, interested stakeholders should work to identify and highlight mutual incentives for working together in the development-cybersecurity narrative, like increasing the efficacy and resilience of good development and reducing the risks for private investors.

Such meetings will become increasingly crucial to apply tools like those discussed in Recommendations #2, #3, and #5 as they are developed.

Recommendation #2: Build a library of credible and politically useful information to present to key development decision makers.

Key to changing discourse to mainstream cybersecurity in development is convincing director-level individuals at development organizations to spend the money necessary. The purpose of this recommendation is to build a body of knowledge pointed at convincing these individuals in key donor organizations the importance of cybersecurity. Identifying and convincing high-level members of the development community enables leverage politics and accountability politics. In order to build more recognition from this portion of the community, cybersecurity advocates must build a library of credible and politically useful information to present to key decision makers. Our research suggests that the two most powerful and useful categories of material are: (1) statistical studies examining on the impact of cybersecurity on development outcomes, and (2) case studies that portray the positive and negative impacts of cybersecurity on development outcomes through storytelling.

Operationalizing Recommendation #2

Actions

- Enable and encourage deep empirical studies on the impact of cybersecurity on development;
- Build a library of examples of impacts and case studies.

What does success look like?

The development of a digital risk and development field, as evidenced by empirical studies on the impact of cybersecurity on all relevant SDGs and academic literature more generally, as well as more articles covering the impact of cyber insecurity on development outcomes. Because these intermediate actions are intended to provide a strong argument to development donors on the importance of cybersecurity, ultimately success is measured in investment dollars in cybersecurity capacity development by donor institutions.

Why is this feasible?

Governments and other funders already provide funding for methodological support and research. However, this giving is not coordinated and generally arrives in small amounts.

How do we make this happen?

The key is in unlocking enough money to build interest around the subject that might entice high profile researchers and journalists to take up the cause. There are a number of ways to raise this money:

- Governments continue investing in themselves through standard mechanisms and encourage private investment;
- Governments invest more money to these causes;
- Governments engage with philanthropies to become more engaged in this topic;
- Appeal to sovereign wealth funds interested in dampening systemic risk;
- Highlight the market value of this research and risk analysis for private companies looking to expand their presence in emerging markets;
- Emphasize the cost-benefits of leveraging donor funds to manage risks by providing seed or matching funding.

Why hasn't it happened yet?

Governments and other funders currently provide funding for methodological support and research. However, this giving is largely uncoordinated and generally arrives in small amounts. In addition, some actors are unwilling to act against their own perceived interest (whether recipients who have had things go wrong or corporations who are keen to gloss over the shortcomings).

Who could lead these efforts?

Public and private donors, think tanks, academia.

Action 2.1: Enable and encourage deep statistical studies on the impact of cybersecurity on development, using the Sustainable Development Goals as a roadmap

A series of statistical studies measuring the correlation of cybersecurity capacity to development outcomes is needed to bridge this gap. In soliciting this work, it is important to remember that the development community's goals extend beyond simply growing GDP and that GDP growth has been largely eschewed by the community as a reliable sole indicator of economic development. In addition, while economic development is important, it is not the only pillar that the community seeks to develop. The SDGs provide a roadmap for the focus of these studies. Individual studies exploring the correlation between cybersecurity capacity and each of the relevant SDGs should be commissioned.

While nonprofits, government agencies, and corporations may hold some capacity to conduct these studies, they will hold the most clout if they originate from well known sources in the development community. Most often, these well

known and respected sources reside in academia. Research grants must be made available by governments and philanthropic organizations to enable this work, and cybersecurity advocates should leverage existing networks to reach and work with influential scholars to develop such studies.[122] Fostering engagement with these leading development thinkers and their understudies is critical to growing a sub-field of development economics examining the relationship between development and cybersecurity.

Action 2.2: Build a library of case studies and examples of the positive and negative impact of cybersecurity on key development outcomes

Hard, quantitative data is not the only kind of empirical evidence that lends authority to good practices and arguments. Indeed, more examples of the harms of cyber insecurity are valuable material for champions of cybersecurity within the development community. But in addition to these anecdotes of harm, advocates need case studies that clearly demonstrate good cybersecurity in development and present the costs and benefits coherently. At least one capacity building institution is currently working on developing a "harm model" to address some of these concerns.

While case research on the topic can certainly take place in think tanks and academia, perhaps the best storytelling ability and the furthest reach resides in journalism. For this reason, governments and philanthropic organizations should join forces to create an independent fellowship program to fund journalists to go to lower-income countries and report on how cybersecurity impacts the development of economies, governance, and society more broadly. Precedent for these types of fellowships exist in the form of programs like the International Reporting Project, which can provide a template for implementation.[123] The GCSCC's existing portal infrastructure could be leveraged to gather these case studies, but it must be acknowledged that the case studies described in this recommendation differ significantly from those compiled by the GCSCC to date.[124]

Recommendation #3: Demystify cybersecurity for aid recipients

Also key to mainstreaming cybersecurity in development is providing tools to enable recipients of development assistance to fold cybersecurity into their development projects. Due to the influence of aid recipients in setting the programmatic and project priorities and agenda, to truly integrate cybersecurity in the development agenda, recipient countries will need to prioritize cybersecurity for investment. This challenge is compounded by the notion that different ministries are often responsible for different parts of the big cybersecurity questions in different governments. For example, sometimes the ministry of defense is most relevant, while other times, the ministry of justice or

the ICT ministry is most active. Each one of these ministries has different priorities and while some ministries may understand the broader challenge, this does not necessarily indicate understanding on the part of the whole government. As we have seen in many higher-income parts of the world, often a whole-of-government approach is needed to address major cybersecurity capacity challenges.

To help these actors and governments better understand the challenge and steps to address cybersecurity in their local context, we recommend investment in the identification of good practices in both cybersecurity and cybersecurity capacity building as well as creation of a toolkit to measure levels of ICT maturity and match those levels of maturity to optimal cybersecurity capacity development.

Operationalizing Recommendation #3

Actions

- Continue working to identify "good practices" that are backed by rigorous empirical study;
- Convene a multistakeholder working group to develop a toolkit for recipient countries to more easily prioritize actions.

What does success look like?

A high-level multistakeholder expert group that is working off the back of empirical research to identify good practices and the creation of a toolkit for use in recipient countries. Ultimately, success rests in better decisions made at the recipient level with regard to how to invest scarce development assistance.

Why is this feasible?

There are models, like the High-Level Expert Groups (HLEGs) convened by the OECD to develop empirically driven good practices in development in the form of the HLEG on the Measurement of Economic Performance and Social Progress.

How do we make this happen?

- Unlock money to provide grants to enable empirically driven research projects to identify good practices
- Key governments apply pressure to the OECD to convene a HLEG on the good practices in managing digital risk in development

Why hasn't it happened yet?

This is a relatively novel problem. There currently is not an academic field that maps to these problems. Furthermore, those who have been tasked with identifying and spreading good practices have not been held to account.

Who could lead these efforts?

The GFCE, OECD, and academia.

Action 3.1: Identify "good practices" that we can empirically prove work

A current shortcoming that plagues the cybersecurity capacity building community is the lack of clearly articulated good practices for cybersecurity (the technical and operational good practices) and cybersecurity capacity building (policy and other interventions that seek to increase the cybersecurity capacity of recipients). Current good practices rely heavily on gut feeling, anecdote, and groupthink. In many cases, these practices, when presented to development practitioners, do not meet certain thresholds for empirical soundness.[125] The cybersecurity capacity building community must take steps to address this problem. While it is true that groups like the Center for Internet Security, the U.S. Department of Commerce's National Institute of Standards and Technology, and the International Standards Organization have produced cybersecurity frameworks, a great deal of work is needed to both test the validity of the recommended interventions and translate them into the local context for recipient countries.

In addition to encouraging more data-driven guidance for cybersecurity good practices, cybersecurity community awareness of and participation in key dialogues in the development community around the use of metrics and identification of good practices in capacity development is crucial. One such dialogue is the OECD's High-Level Expert Group (HLEG) on the Measurement of Economic Performance and Social Progress.[126] These conversations hold value for the cybersecurity community in two ways. First, they are an opportunity to raise the importance of cybersecurity in development. Second, and perhaps as crucially, they provide visibility into good practice in capacity development, which could provide insight for those attempting to gather good practices in cybersecurity capacity building. Programs like the HLEG are important opportunities for the cybersecurity community to engage with the development community.

Finally, the cybersecurity capacity building community must identify capacity building interventions that they can empirically prove have the desired impact. The Global Forum on Cyber Expertise (GFCE) project on global good practices is a step in the right direction for the articulation of cybersecurity capacity building good practices.[127] However, arguably this forum and others are simply exacerbating the groupthink problem with good practices, as the majority of

collection focuses on what people and organizations are doing rather than answering the more difficult question of whether any of this is actually working or will continue to work as the technology and environment changes. Any process to identify and communicate good practices in cybersecurity and cybersecurity capacity building needs to be backed by evidence or empirics. Small, data-driven experiments and projects, like the work of CyberGreen to identify good practices in DDoS prevention and mitigation must be enabled on a broader scale.[128]

Ultimately, the GFCE would be a good hub for these activities, though the institution is under-resourced and may lack some of the methodological capacity to do so on its own. Thus, moving forward, in order to mainstream these practices in development, the OECD may be the best organization to shepherd a working group to develop good practices in managing digital risk in development, in association with the GFCE. Member governments should apply pressure to the OECD to create such an HLEG to run in parallel with or follow the ongoing HLEG on empirically driven good practices in development, which is due to culminate with a final report, to be released in late November 2018.

Action 3.2: Develop a toolkit to enable bottom-up agenda setting

The cybersecurity capacity building community needs to create toolkits to enable informed consumption on the part of aid recipients and facilitate bottom-up agenda setting. Key organizations should develop a multi-stakeholder consultative process to develop such a toolkit.

Where current tools aimed at this goal—like the maturity models mentioned earlier in this report—focus on highlighting the cybersecurity capacity of countries, a different kind of toolkit is needed. This toolkit should focus on measuring the ICT maturity of a country (rather than cybersecurity maturity) and identify primary threats to important assets then use these factors to identify priority cybersecurity competencies. These cybersecurity benchmarks should be closely tied to good practices in cybersecurity. Such a framework should build on existing resources, including ones developed for other fields, like the Nottingham Strategic ICT toolkit project,[129] and cybersecurity-specific ones, like the Cyber Readiness Index.[130]

This type of framework serves two primary purposes. First, it gives potential ministers in charge of implementing ICT and cybersecurity projects and policies a menu of benchmarks to work towards. Second, it provides guidance on how to prioritize which benchmarks are most important given the local context, an important aspect currently missing from other frameworks and models.[131] Certain cybersecurity capacities are necessary in some, but not all, contexts. While it is important to move all countries towards better cybersecurity, these improvements will happen incrementally. Put simply, different countries will

need to prioritize or give more urgent attention to building cybersecurity capacities that meet their current needs.

Whereas the OECD emerges as a logical host for the expert group on managing digital risk in development, the host and sponsor of this multistakeholder process is less clear. Candidates include the GFCE, which may be well suited, as well as the World Bank itself, other UN agencies, a coalition of willing bilateral aid agencies, and existing nongovernmental organizations like the Internet Governance Forum.

Recommendation #4: Bring more cybersecurity expertise into donor institutions

Integrating cybersecurity expertise in donor institutions will be crucial to mainstreaming cybersecurity in development. However, getting the precise nature of this cybersecurity expertise right is important. Donor institutions do not require deep technical experts. Instead they need what amounts to consultants who can work in recipient countries to help turn aid recipients into more informed customers of ICT and cybersecurity products. This will only be possible if key individuals at the director level and above are convinced of the importance of cybersecurity to deliver on their goals and are willing to advocate for more in-house expertise (see Recommendation #2).

Operationalizing Recommendation #4

Actions

- Explore short-term solutions like fellowships.
- Leverage funding mechanisms to create long-term cybersecurity portfolios in major financial institutions.

What does success look like?

Ultimately, success in this project comes in the form of cybersecurity capacity building experts (as described above) in all donor institutions. In large institutions, like the World Bank, the presence of cybersecurity expertise in either (a) each of the thematic practice areas or (b) regional units is necessary.

Why is this feasible?

The Israeli government is leading the way by providing a fund and seconding an employee into the InterAmerican Development Bank to focus on cybersecurity. More national governments could follow suit in other regional development banks, as well as globally focused institutions like the World Bank and the International Monetary Fund.

How do we make this happen?

Key funding governments and private organizations need to pressure donor institutions to spend money on improving the state of cybersecurity expertise in those institutions. This could include placing limited conditions on IDA contributions (in the case of governments) and the creation of cybersecurity-themed trust funds in groups like the World Bank's DFi.

Why hasn't it happened yet?

As with many of the previous recommendations, the novelty of cybersecurity contributes to this problem. In addition, like any set of large institutions, major development institutions are bureaucratic structures that can take a great deal of time to change. While some in these structures have been advocating for this exact change for years, it has not yet taken hold.

Who could lead these efforts?

Donor governments and private donors

Development donors, who in large part help craft projects and programs, must recruit, develop, and retain the internal expertise to make sure that recipients of aid money are informed customers when it comes to the use of technology and are able to identify risks and take steps to manage them. In at least one major development finance institution, the existence of a stable, long-term (five or more years) portfolio triggers the ability to hire more staff. Thus, if cybersecurity's profile rises in the development community, this challenge could resolve itself. However, there are levers policy and decision makers can pull to both infuse donor institutions with more cybersecurity expertise in the short-term and develop longer term portfolios.

Action 4.1: Explore short-term solutions like fellowships and secondments

In the sorter term, development institutions should explore the potential of fellowships following the model of the Presidential Innovation Fellowship in the U.S., or the Agentes de Innovacion in Mexico, designed to bring more technological expertise into areas of public service, as well as expert secondments from donor governments. A successful fellowship program would need to be funded by a public or private donor and link fellows directly to full-time staff or offices with institutional knowledge. Linking to staff or an office has two benefits: it enables a fellow to better navigate a complex bureaucracy and institutionalizes any lessons learned or activities undertaken by the fellow beyond the fellow's term. The benefit of fellowships is that they are cheap in comparison to creating a long-term portfolio, as described below. In addition, a roster of available experts could be compiled to ease the burden of finding short-

term contractors, fellows, or secondees. A common roster serving several institutions would reduce the time to find expertise in the market and facilitate the experts' understanding of the framing of their mission (cybersecurity and development).

Action 4.2: Leverage funding mechanisms to create long-term cybersecurity portfolios in major donor institutions

To create more long-term, sustainable programs, public and private funders should leverage funding mechanisms like trust funds and donation conditions. The establishment of cybersecurity themed multilateral or public-private trust funds at major financial institutions would provide the sustained funding needed to begin hiring the right experts. It is crucial that the money not only be made available, but also that it is spent wisely. Spending on the creation of a cybersecurity specific team may lead to stovepiping of the issue in a manner more akin to prioritization as described in Chapter 2. Instead of creating a separate cybersecurity practice, the ultimate goal for major donor institutions should be to create a system or team that places digital risk advisors on every implementation team, like the World Bank's CPF and SCD teams.

Recommendation #5: Create and implement digital risk impact assessments for development projects and programs

A key vehicle for mainstreaming issues like environmentalism, social impact, and human rights in development has been the creation and implementation of impact assessments. These movements and impact assessments provide a model for cybersecurity to emulate. However, as suggested in Recommendation #1, framing is crucial. Rather than securitizing the assessments, they should focus on identifying digital risk.

Operationalizing Recommendation #5

Actions

Create and implement digital risk impact assessments for development projects and programs.

What does success look like?

As with human rights before it, success in this endeavor would result in the use of digital risk impact assessments in all development projects incorporating an element of ICT in their programming.

Why is this feasible?

Precedent for this type of impact assessment exists in other areas that represent cross-cutting or systemic risk, like human rights and the environment.

How do we make this happen?

The creation of a working group to identify frameworks for cybersecurity impact assessments based off of HRIAs, environmental impact assessments, and other existing impact assessments.

Who could lead these efforts?

The World Bank, the World Economic Forum, the GFCE, the Global Commission on the Stability of Cyberspace

The development community long ago learned how to address risks to the environment, human rights, and social welfare. Digitization presents new risks that can both worsen existing risks and pose novel ones of its own. Therefore, models from the past could be adapted and applied to the context of cyber risk management. This risk framework should be geared towards assisting beneficiaries of development spending to better understand and manage the risks of digitization on a project by project basis. Taking cues from both HRIAs and the World Bank's Environmental and Social Framework, digital risk impact assessments (DRIA) should draw on good practices in digital risk management and mitigation and be customizable to different industries and projects. As with the toolkit proposed in Recommendation #3.2, a DRIA should draw on existing models and tools.

The exact shape of a DRIA framework should be developed through a multistakeholder working group housed in an existing institution like the GFCE, the Global Commission on the Stability of Cyberspace, the World Economic Forum, or the Internet Governance Forum.

Conclusion

Although the lights went out again in parts of Ukraine in December 2016,[132] December 2017 saw the lights (and heat) stay on. The 2015 and 2016 incidents served as a major wake-up call for policy makers. In response to the challenges facing their rapidly digitizing infrastructure—and specifically in response to the 2015 attack on their power grid—Ukraine adopted a National Cybersecurity Strategy to help identify how to create "the conditions that ensure safe cyberspace and its use."[133] Working with partner governments, Ukraine built a National Cybersecurity Coordination Center. Working with a Cyber Defence Trust Fund through the North Atlantic Treaty Organization (NATO), the Ukrainian government was able to "enhance the country's technical capabilities" to "counter cyber threats."[134]

What you have here is an example of proof that an impact can be made. But in a way Ukraine is fortunate. Many in the West view Ukraine as region of strategic importance and are therefore willing to invest heavily in securing its critical infrastructure from foreign adversaries. Not every country is so lucky. Indeed, military investment is both less likely to flow to countries of lower strategic importance and less likely to focus on securing digital systems not deemed critical for national defense but that may be nonetheless critical for broader development objectives. If this work is left to militaries, development will be selective and uneven, creating problems that undermine the achievement of development goals and could be avoided. If lower- and middle-income states continue to be neglected or neglect investing in cybersecurity they risk undoing and undermining much of the progress and potential that digital technology promises for improving the conditions of their people. Against this backdrop, several key findings emerge.

First, the community implementing digitization and connectivity projects exists quite separately from the community attempting to develop the capacity to ensure the reliability, resilience, and trustworthiness of these newly implemented digital systems and the internet more broadly. Bridging the gap between these two communities will be critical for managing the present and future risks to the development of lower- and middle-income countries.

Second, and relatedly, concepts of cybersecurity and cyber risk management must be mainstreamed in the development community. Bridging the gap between the cybersecurity capacity building community and the development community will help deliver this outcome, but other steps could and should be taken to equip the development community for success in helping their beneficiaries better manage cyber risks.

Third, some of the reluctance to mainstream cybersecurity in international development on the part of donors is well founded. Other development equities

will at times legitimately outweigh the need for investment in cybersecurity. In addition, the cybersecurity capacity building community could do more to prove the value of its interventions through empirical examinations of good practices in cybersecurity capacity building.

Fourth, more needs to be done to demystify cybersecurity for aid recipients, who play a major role in deciding how to invest development funds. A framework is needed to help decision and policy makers understand what cybersecurity capacity building activities to prioritize and when. Cybersecurity maturity models, like the Oxford Global Cyber Security Capacity Center's, are a step in the right direction but were not originally intended to provide such a decision-making framework.

This report has tried to illuminate key reasons why cybersecurity should be mainstreamed in international development, key challenges to doing so, and key steps to overcome those challenges. This work, however, is just a start and one of the crucial findings of this report is simply that a great deal more research is needed. Understanding the impact of cyber insecurity on development is critical to building a strong case that major development funders and implementers should heed the warnings of the cybersecurity community and bake cyber risk management considerations into their projects from the beginning.

Appendix: The SDGs and Cybersecurity

This table is built on reflections by the author, interviewees, and reviewers of this report. It also draws insight from the findings of Internet Governance Forum 2017's Best Practice Forum on Cybersecurity.[135] Rather than a finished product, this table should be considered a work in progress, to be built upon by any and all interested parties. The author welcomes any additional thoughts from readers of this report.

Goal #1: End Poverty

Notable targets

- Reduce by half the number of humans living in poverty by 2030
- Give the poor and vulnerable equal rights to economic resources
- Reduce the vulnerability of the poor and other vulnerable populations to economic, social and environmental shocks and disasters

How good cybersecurity contributes to the goal

- Supports economic growth by preserving the benefits digitization and increasing trust in it.
- Ending poverty depends on individuals being able to access information over the Internet. Thus, it can be disrupted by weaknesses in, and attacks on, the availability of information services and the networks that individuals use in connecting to them.

Goal #2: Zero Hunger

Notable targets

- Correct and prevent distortions in the world agricultural markets
- Adopt measures to ensure the proper functioning of food commodity markets and their derivatives and facilitate timely access to market information

How good cybersecurity contributes to the goal

- While famine has more significant underlying causes, a stable food supply relies on distribution mechanisms, which relies on dependable ICT

Goal #3: Good Health and Well Being

Notable targets

- By 2030, reduce the global maternal mortality ratio to less than 70 per 100,000 live births. By 2030, reduce by one third premature mortality from non-communicable diseases through prevention and treatment and promote mental health and well-being
- Achieve universal health coverage, including financial risk protection, access to quality essential health-care services and access to safe, effective, quality and affordable essential medicines and vaccines for all

How good cybersecurity contributes to the goal

- Increased digitization of the healthcare sector yields immediate dividends, but also exposes patient data to new risks and opens hospitals and other service providers up to new risk for disruption, as demonstrated by the 2017 ransomware attacks

Goal #4: Quality Education

Notable targets

- Substantially increase the number of youths and adults who have relevant skills, including technical and vocational skills, for employment, decent jobs and entrepreneurship
- Build and upgrade education facilities that are child, disability, and gender sensitive and provide safe, nonviolent, inclusive and effective learning environments for all

How good cybersecurity contributes to the goal

- ICT allows for more distributed and scalable delivery of educational products. However, these products and the systems must be trusted and secure to safeguard the privacy of students
- Additionally, good practices when using computers and digital technologies will be increasingly important skills, and educating populations on good cyber hygiene is an integral part of that

Goal #5: Gender Equality

Notable targets

- End all forms of discrimination against all women and girls everywhere
- Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation
- Undertake reforms to give women equal rights to economic resources, as well as access to ownership and control over land and other forms of property, financial services, inheritance and natural resources, in accordance with national laws

How good cybersecurity contributes to the goal

- Although literature is still nascent on the topic, some studies have suggested that cybersecurity inequalities exacerbate existing societal inequalities, including along gender lines. In addition, online resources for reporting discrimination and violence against women require strict privacy controls or they risk putting women at further risk

Goal #6: Clean Water and Sanitation

Notable targets

- Expand international cooperation and capacity-building support to developing countries in water- and sanitation-related activities and programmes, including water harvesting, desalination, water efficiency, wastewater treatment, recycling and reuse technologies

- Support and strengthen the participation of local communities in improving water and sanitation management

How good cybersecurity contributes to the goal

- Cybersecurity is important for protecting critical systems that use IT. As evidenced by various hacks on critical infrastructure, water and sanitation systems, as well as energy grids, are not out of bounds

Goal #7: Affordable and Clean Energy

Notable targets

- Expand infrastructure and upgrade technology for supplying modern and sustainable energy services for all in developing countries, in particular least developed countries, small island developing States, and landlocked developing countries, in accordance with their respective programmes of support

How good cybersecurity contributes to the goal

- Affordable and clean energy increasingly relies on automation and automated systems. As portrayed by power disruptions in Ukraine, these systems are vulnerable and can present new avenues for disruption is not properly secured

Goal #8: Decent Work and Economic Growth

Notable targets

- Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation, and encourage the formalization and growth of micro-, small- and medium-sized enterprises, including through access to financial services
- Achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive sectors
- Strengthen the capacity of domestic financial institutions to encourage and expand access to banking, insurance and financial services for all

How good cybersecurity contributes to the goal

- Refer to Goal 1. Economic growth depends on things like your money staying in the bank when you put it there, ensuring you control your intellectual property, and that the systems you use for your business are available.
- Mobile payment systems are increasingly important for distributed access to financial flows. Insecure payment systems will undermine trust and potentially stunt economic growth

Goal #9: Industry, Innovation, and Infrastructure

Notable targets

- Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all
- Increase the access of small-scale industrial and other enterprises, in particular in developing countries, to financial services, including affordable credit, and their integration into value chains and markets
- Upgrade infrastructure and retrofit industries to make them sustainable, with increased resource-use efficiency and greater adoption of clean and environmentally sound technologies and industrial processes, with all countries taking action in accordance with their respective capabilities
- Facilitate sustainable and resilient infrastructure development in developing countries through enhanced financial, technological and technical support to African countries, least developed countries, landlocked developing countries and small island developing States
- Support domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification and value addition to commodities
- Significantly increase access to information and communications technology and strive to provide universal and affordable access to the internet in least developed countries by 2020

How good cybersecurity contributes to the goal

- Increased access to ICT and novel internet-connected technologies without managing the technologies' security risks making them inconvenient and may hinder uptake.
- Ports and modern transportation infrastructure have proven vulnerable to disruption from cyberattacks.

Goal #10: Reduced Inequalities

Notable targets

- Empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status
- Ensure equal opportunity and reduce inequalities of outcome, including by eliminating discriminatory laws, policies and practices and promoting appropriate legislation, policies and action in this regard

How good cybersecurity contributes to the goal

- Protecting the integrity of people's information should be a priority no matter if it is the poor or the rich and powerful. Uneven access to cyber tools disadvantages the poor and exacerbates inequalities

Goal #11: Sustainable Cities and Communities

Notable targets

- By 2030, provide access to safe, affordable, accessible and sustainable transport systems for all, improving road safety, notably by expanding public transport, with special attention to the needs of those in vulnerable situations, women, children, persons with disabilities and older persons
- By 2030, significantly reduce the number of deaths and the number of people affected and substantially decrease the direct economic losses relative to global gross domestic product caused by disasters, including water-related disasters, with a focus on protecting the poor and people in vulnerable situations

- By 2020, substantially increase the number of cities and human settlements adopting and implementing integrated policies and plans towards inclusion, resource efficiency, mitigation and adaptation to climate change, resilience to disasters, and develop and implement, in line with the Sendai Framework for Disaster Risk Reduction 2015-2030, holistic disaster risk management at all levels
- Support least developed countries, including through financial and technical assistance, in building sustainable and resilient buildings utilizing local materials

How good cybersecurity contributes to the goal

- Smart cities with intelligent physical, social, institutional, and economic architecture help deliver greater sustainability to cities and communities and contribute to the targets outlined here. However, as EY notes, insecure hardware, a larger cyber attack surface, issues around internet bandwidth, and increased reliance on apps are all cybersecurity challenges faced by increasingly digitized cities and communities.[136]

Goal #16: Peace, Justice, and Strong Institutions

Notable targets

- Significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime
- Substantially reduce corruption and bribery in all their forms
- Develop effective, accountable and transparent institutions at all levels
- Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements
- Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime

How good cybersecurity contributes to the goal

1. Information systems can be a boon for transparency and increase the strength of peace and justice institutions. However, just as these systems can improve the delivery of justice, malicious manipulation of information and data threatens to weaken core democratic institutions.
2. Due to low barriers to entry and high yields, organized criminal groups are increasingly engaging in cybercrime. Equipping lower- and middle-

income countries with the expertise to combat this new form of crime will help safeguard populations from this activity and give police the capacity to identify and prosecute cybercrime

Notes

1 Robert M. Lee, Michael J. Assante, and Tim Conway. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case." *E-ISAC*. March 18. p1. .

2 Laszlo Lovei. 1998. "Electricity Reform in Ukraine." *P ublic Policy for the Private Sector*. Note No. 168. December..Christina Maciw, Natalie Bell, and Vitaliy Radchenko. 2009. "Ukraine Prepares 15 Oblenergos for Privatisation." *Mondaq*. August 13. .

3 Vitaliy Radchenko, Olexander Martinenko, and Inna Antipova. 2015. "CMS guide to electricity - Ukraine." *C ameron McKenna Nabarro Olswang LLP*. September 1. .

4 World Bank. 2012. "Expanding the Ukrainian Power Transmission Grid." *World Bank*. February 9. .

5 World Bank. "Electric power transmission and distribution losses (% of output)." *World Bank - IEA Statistics*. Accessed March 19, 2018. .

6 Melissa Hathaway. 2018. "Managing National Cyber Risk." *The Organization of American States*. Forthcoming.

7 The Guardian. 2016. "Massive cyber-attack grinds Liberia's internet to a halt." *The Guardian*. November 3. .

8 Nigerian Communications Commission. "Effects of Cybercrime on Foreign Direct Investment and National Development." *Nigerian Communications Commission*. .

9 Zetter, Kim. 2016. "That Insane, $81m Bangladesh Bank Heist? Here's what we know." *WIRED*. May 17. .

10 In addition to running Dragos Inc., a cybersecurity company, Robert M. Lee is a Cybersecurity Policy Fellow with New America's Cybersecurity Initiative.

11 VICELAND. 2016. "Did Russia Hack Ukraine's Electrical Grid?" *VICELAND.* November 30.. 2:00 - 4:00. .

12 Andy Greenberg. 2017. "Watch Hackers Take Over the Mouse of a Power-Grid Computer." *WIRED*. June 20. .

13 VICELAND. 2016. "Did Russia Hack Ukraine's Electrical Grid?" *VICELAND.* November 30. 2:00 - 4:00. .

14 Robert M. Lee, Michael J. Assante, and Tim Conway. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case." *E-ISAC*. March 18. p2. .

15 World Bank. 2016. "World Development Report 2016: Digital Dividends." *World Bank*. January. p3. .

16 Sandra Sargent. 2017. "World Bank Donor Perspective on Cyber Security." *Commonwealth Telecommunications Organisation.* .

17 Pawlak, Patryk. 2014. "Riding the Digital Wave – Introduction." *EU Institute for Security Studies*. December. p6. .

18 Pawlak, Patryk. 2014. "Riding the Digital Wave – Introduction." *EU Institute for Security Studies*. December. p12. .

19 Internet Society. 2017. "A policy framework for an open and trusted internet." *Internet Society.* March..

20 Internet Governance Forum. 2017. "IGF 2017 - Best Practice Forum on Cybersecurity." *Internet Governance Forum*. .

21 Internet Society. 2017. "A policy framework for an open and trusted internet." *Internet Society.* March..

22 Department for International Development. 2018. "Digital Strategy 2018-2020: Doing Development in a Digital World." *Department for International Development*. January. p7. .

23 World Bank. 2016. “World Development Report 2016: Digital Dividends.” *World Bank*. January. p2. .

24 World Bank. 2016. “World Development Report 2016: Digital Dividends.” *World Bank*. January. p3. .

25 United Nations. 2017. “The Sustainable Development Goals Report 2017.” *United Nations.* .

26 United Nations. “Sustainable Development Goal 1.” *United Nations.* .

27 United Nations. “Sustainable Development Goal 8.” *United Nations.* .

28 James Manyika and Charles Roxburgh. 2011. “The great transformer: The impact of the Internet on economic growth and prosperity.” *McKinsey Global Institute*. October. p3. .

29 ibid.

30 Center for Strategic and International Studies. 2014. “Net Losses: Estimating the Global Cost of Cybercrime.” *Center for Strategic and International Studies*. June. .

31 United Nations. “Sustainable Development Goal 10.” *United Nations*. .

32 Internet Governance Forum. 2017. “IGF 2017 - Best Practice Forum on Cybersecurity.” *Internet Governance Forum*. .

33 United Nations. “Sustainable Development Goal 9.” *United Nations*. .

34 Claus Herbolzheimer and Max-Alexander Borreck. 2017. “Time for Transportation & Logistics To Up Its Cybersecurity As Hackers Put It On Target List.” *Forbes*. June 28. .

35 United Nations. “Sustainable Development Goal 16.” *United Nations*.

36 United Nations. “Sustainable Development Goal 11.” *United Nations*. .

37 Shelley Singh. 2018. “How safe is Digital Intia?” *The Economic Times*. January 14. .

38 Lily Hay Newman. 2017. “The Ransomware Meltdown Experts Warned About is Here.” *WIRED*. May 12. .

39 Andy Greenberg. 2017. “‘Crash Override’: The Malware That Took Down a Power Grid.” *Wired*. June 12. .

40 Michael Corkery. 2016. “Hackers’ $81 Million Sneak Attack on World Banking.” *New York Times*. April 20. .

41 Robert M. Lee, Michael J. Assante, and Tim Conway. 2016. “Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case.” *E-ISAC*. March 18. .

42 Kim Zetter. 2017. “The Ukrainian Power Grid Was Hacked Again.” *Motherboard.* January 10. .

43 India Today. 2017. “WannaCry did hit India and even central govt portal. So why did Centre downplay the ransomware attack?” *India Today*. June 19. .

44 Principles for Digital Development. “Principles.” *Principles for Digital Development.* .

45 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2015. “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” *United Nations.* July 22. p11..

46 United Nations. “Millenium Development Goals.” *United Nations*. .

47 United Nations. “Sustainable Development Goals.” *United Nations*. .

48 Dorothea Kleine and Tim Unwin. 2009. “Technological Revolution, Evolution and New

Dependencies: What's New about ICT4D?" *Third World Quarterly*. Vol. 30, No. 5. p1049. .

49 World Bank. 2013. "Human Rights Impact Assessments: A Review of Literature, Differences with other forms of Assessments and Relevance for Development." *World Bank.* February. p1. .

50 ibid.

51 United Nations. 2005. "Secretary-General Appoints John Ruggie of United States Special Representative on Issue of Human Rights, Transnational Corporations, Other Business Enterprises." *United Nations*. July 28. .

52 World Bank. 2013. "Human Rights Impact Assessments: A Review of Literature, Differences with other forms of Assessments and Relevance for Development." *World Bank.* February. pXI. .

53 This is not an exhaustive list of actors that fall under this category, but instead a sample of such actors to illustrate the types of institutions and organizations that might be included in each category.

54 World Bank. "Who We Are." *World Bank*. .

55 The International Bank for Reconstruction and Development

56 The International Development Association

57 The International Finance Corporation

58 The Multilateral Investment Guarantee Agency

59 The International Centre for Settlement of Investment Disputes

60 World Bank. "Who We Are." *World Bank*. .

61 World Bank. "What We Do." *World Bank*. .

62 World Bank. "Who We Are - IBRD." *World Bank*. .

63 World Bank. "Development Finance (DFi)." *World Bank*. .

64 Interview with the author. Conducted February 2018.

65 World Bank. "Reimbursable Advisory Services." *W orld Bank*. .

66 World Bank. 2012. "Getting to Know the World Bank." *World Bank.* July 26.

67 World Bank. "How Does IDA Work?" *World Bank.* .

68 Bretton Woods Project. 2010. "IDA replenishment." *Bretton Woods Project*. February 15. .

69 World Bank. 2017. "Fact Sheet on World Bank Trust Funds." *World Bank*. April 18. .

70 Joseph E. Stiglitz. 2017. "The Measurement of Economic Performance and Social Progress." *Internati onal Economic Association World Congress*. June 19. p8. https://www8.gsb.columbia.edu/faculty/jstiglitz/sites/jstiglitz/files/The%20Measurement%20of%20Economic%20Performance%20and%20Social%20Progress.pdf.

71 Joseph E. Stiglitz. 2017. "The Measurement of Economic Performance and Social Progress." *Internati onal Economic Association World Congress*. June 19. p20. https://www8.gsb.columbia.edu/faculty/jstiglitz/sites/jstiglitz/files/The%20Measurement%20of%20Economic%20Performance%20and%20Social%20Progress.pdf.

72 Simon Kuznets. 1934. "National Income, 1929-1932." *National Bureau of Economic Research*. Bulletin 49. June 7. p1. .

73 OECD. 2012. "Nobel Laureate Professor Joseph Stiglitz emphasises need for alternative measures of well being at 4th OECD World Form." *OECD*. October 17. .

74 Gernot Kohler and Emilio José Chaves. 2003. *Glob alization: Critical Perspectives.* Nova Science Publishers, Inc. New York. p336.

75 Simon Kuznets. 1934. "National Income, 1929-1932." *National Bureau of Economic Research*. Bulletin 49. June 7. p12. .

76 Joseph Stiglitz. 2009. "GDP Fetishism." *Project Syndicate*. September. .

77 Interview with the author. Conducted October 2017.

78 Pijnenburg Muller, Lilly. 2015. "Cybersecurity Capacity Building in Developing Countries: Challenges and Opportunities." *Norwegian Institute of International Affairs*. p10. .

79 This is not an exhaustive list of actors that fall under this category, but instead a sample of such actors to illustrate the types of institutions and organizations that might be included in each category.

80 GFCE Secretariat. 2017. "GFCE Member Survey 2017." *Global Forum on Cyber Expertise*.

81 These numbers are based on interviews with the author and do not constitute an authoritative number. The GFCE is currently undergoing a process to identify an accurate estimate of cybersecurity capacity building spending globally. The US$1 billion estimate appears to be a high-end outlier with the majority of estimates clustered between US$100 million and US$300 million.

82 OECD. 2018. "Total official and private flows." *OEC D*. .

83 Alexander Klimburg and Hugo Zylberberg. 2015. Cybersecurity Capacity Building: Developing Access. *Norwegian Institute of International Affairs*. p20. .

84 Alexander Klimburg and Hugo Zylberberg. 2015. Cybersecurity Capacity Building: Developing Access. *Norwegian Institute of International Affairs*. p20-39. .

85 Computer emergency response team (CERT) and computer security incident response team (CSIRT) are terms used interchangeably in the cybersecurity world. These teams have been likened to digital fire brigades and fill a number of different roles. For more information on CERTs/CSIRTs, see: Isabel Skierka, Robert Morgus, Mirko Hohmann, and Tim Maurer. 2015. "CSIRT Basics for Policy-Makers." *Transatlantic Digital Debates.* May. .

86 Global Cyber Security Capacity Centre. "Cybersecurity Capacity Portal." *University of Oxford.* .

87 Global Cyber Security Capacity Centre. "Global Cyber Capacity Building at a Glance." *University of Oxford.* .

88 Craig Timberg. 2015. "Net of Insecurity: A Flaw in the Design." *Washington Post.* May 30. .

89 Craig Timberg. 2015. "Net of Insecurity: A Flaw in the Design." *Washington Post.* May 30. .

90 OECD. "Official development assistance - definition and coverage." *OECD*. .

91 For a deeper examination of ODA and cybersecurity, see: Alexander Klimburg and Hugo Zylberberg. 2015. Cybersecurity Capacity Building: Developing Access. *Norwegian Institute of International Affairs*. p41-45. .

92 Sami Saydjari. 2018. "Engineering Trustworthy Systems". *McGraw-Hill*. (Forthcoming).

93 Patryk Pawlak. 2014. "Riding the Digital Wave – Introduction." *EU Institute for Security Studies*. December. p15. .

94 World Bank. 2016. "World Development Report 2016: Digital Dividends." *World Bank*. January. p224. .

95 Patryk Pawlak. 2014. "Riding the Digital Wave – Introduction." *EU Institute for Security Studies*. December. p15. .

96 William H. Dutton, Sadie Creese, Ruth Shillair, Maria Bada, and Taylor Roberts. 2017. "Cyber Security Capacity: Does It Matter?" *Quello Center*. Working Paper No. 2938078. March 23. p8-16..

97 William H. Dutton, Sadie Creese, Ruth Shillair, Maria Bada, and Taylor Roberts. 2017. "Cyber Security Capacity: Does It Matter?" *Quello Center*. Working Paper No. 2938078. March 23. p21..

98 Sandra Sargent. 2017. "World Bank Donor Perspective on Cyber Security." *Commonwealth Telecommunications Organisation*. .

99 World Bank. 2016. "World Development Report 2016: Digital Dividends." *World Bank*. January. p69-70. .

100 Interview with the author. Conducted October 2018.

101 Global Cyber Security Capacity Centre. 2017. "Cybersecurity Capacity Maturity Model for Nations (CMM)." *University of Oxford*. February 9. .

102 Melissa Hathaway. 2015. "Cyber Readiness Index 2.0." *Potomac Institute for Policy Studies*. November. .

103 Fergus Hanson, Tom Uren, Fergus Ryan, Michael Chi, Jack Viola, and Eliza Chapman. 2017. "Cyber Maturity in the Asia Pacific Region 2017." *Australian Strategic Policy Institute*. December 12. .

104 Andrea Cornwall and Deborah Eade. 2010. "Deconstructing Development Discourse: Buzzwords and Fuzzwords." *Practical Action Publishing*. .

105 Andrea Cornwall and Deborah Eade. "Deconstructing Development Discourse: Buzzwords and Fuzzwords." *Practical Action Publishing*. p2. .

106 See, for example:Department for International Development. 2013. "Glossary of terms used by the Department for International Development." *UK Department for International Development*. August 13. .US AID. 2014. "Glossary of ADS Terms." *USAID*. April 30. .J. Brian Atwood. 2012. "Development Co-operation Report 2012: Lessons in Linking Sustainability and Development. *OECD Publishing*. .Wolfgang Sachs. 2010. "The Development Dictionary n. A Guide to Knowledge as Power." *Zed Books*. .

107 Interview with the author. Conducted October 2017.

108 World Bank. 2017. "Our Work." *World Bank*. .

109 The Center for Cyber Safety and Education. 2017. "2017 Global Information Security Workforce Study." *Fr ost & Sullivan*. p2. .

110 The Center for Cyber Safety and Education. 2017. "2017 Global Information Security Workforce Study." *Fr ost & Sullivan*. p3. .

111 The Center for Cyber Safety and Education. 2017. "2017 Global Information Security Workforce Study." *Fr ost & Sullivan*. p4. .

112 The Center for Cyber Safety and Education. 2017. "2017 Global Information Security Workforce Study." *Fr ost & Sullivan*. p6. .

113 Interview with the author. Conducted October 2017.

114 Interview with the author. Conducted October 2017.

115 Margaret E. Keck and Kathryn Sikkink. 1998. "Activists Beyond Borders: Advocacy Networks in International Politics." Cornell University Press: Ithaca, NY.

116 Margaret E. Keck and Kathryn Sikkink. 1998. "Activists Beyond Borders: Advocacy Networks in International Politics." Cornell University Press: Ithaca, NY. p2.

117 Margaret E. Keck and Kathryn Sikkink. 1998. "Activists Beyond Borders: Advocacy Networks in

International Politics." Cornell University Press: Ithaca, NY.

118 Margaret E. Keck and Kathryn Sikkink. 1998. "Activists Beyond Borders: Advocacy Networks in International Politics." Cornell University Press: Ithaca, NY. p16.

119 Pawlak, Patryk. 2014. "Riding the Digital Wave." *E U Institute for Security Studies*. December. .

120 Alexander Klimburg and Hugo Zylberberg. 2015. Cybersecurity Capacity Building: Developing Access. *Norwegian Institute of International Affairs*. p45. .

121 Troy Hunt. 2018. "Is India's Aadhaar System Really 'Hack-Proof'? Assessing a Publicly Observable Security Posture." *troyhunt.com*. January 11. .

122 Such scholars include the likes of Kaushik Basu at Cornell University, Olivier Blanchard and Esther Duflo at Massachusetts Institute of Technology, Paul Collier at Oxford University, Paul Krugman at the City University of New York, WIlliam Easterly and Paul Romer at New York University, Justin Yifu Lin at Peking University, Martin Ravallion at Georgetown University, John Ruggie and Amartya Sen at Harvard University, and Joseph Stiglitz and Jeffrey Sachs at Columbia University.

123 International Reporting Project. "About the IRP." *I nternational Reporting Project*. .

124 Global Cyber Security Capacity Centre. "Cybersecurity Capacity Portal - Case Study." *Universit y of Oxford*. .

125 For one example of a study on evidence-based practice in the development community, see: USAID. 2016. "Strengthening Evidence-Based Development: Five years of better evaluation practice at USAID 2011-0216." *USAID*. March. .

126 OECD. "High Level Expert Group on the Measurement of Economic Performance and Social Progress." *OECD*. .

127 GFCE. "Global Good practices identified by the GFCE community." *Global Forum on Cyber Expertise*. Which.

128 Cyber Green. "What We Do." *Cyber Green*. .

129 The University of Nottingham. "Strategic ICT toolkit." *University of Nottingham*. .

130 Melissa Hathaway. 2015. "Cyber Readiness Index 2.0." *Potomac Institute for Policy Studies*. November. .

131 It should be noted that teams associated with both the Cyber Readiness Index and the Oxford Maturity Model work with countries to tailor local strategies using their respective tools as frameworks. However, both of these tools require additional hands-on expertise and are of limited utility to policymakers in recipient countries on their own.

132 Andy Greenberg. 2017. "'Crash Override': The Malware That Took Down A Power Grid." *WIRED*. June 12. .

133 Oleksii Tkachenko. 2017. "Cybersecurity in Ukraine: National Strategy and international cooperation." *Global Forum on Cyber Expertise*. July 6. .

134 Oleksii Tkachenko. 2017. "Cybersecurity in Ukraine: National Strategy and international cooperation." *Global Forum on Cyber Expertise*. July 6. .

135 Internet Governance Forum. 2017. "IGF 2017 - Best Practice Forum on Cybersecurity." *Internet Governance Forum*. .

136 Ernst & Young LLP. 2016. "Cyber Security A necessary pillar of Smart Cities." *Ernst & Young*. .

This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America's work, or include our content in derivative works, under the following conditions:

• **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit **creativecommons.org**.

If you have any questions about citing or reusing New America content, please visit **www.newamerica.org**.

All photos in this report are supplied by, and licensed to, **shutterstock.com** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.