



Digital Inclusion and a Trusted Internet

The Role of the International Development Community in Balancing Internet Access and Cybersecurity

Jonathan Dolan
October 2018





CENTER FOR DIGITAL ACCELERATION

The Center for Digital Acceleration helps our clients integrate digital tools and approaches across their portfolio through research, design, and implementation. Our work covers a cross section of sectors including health, governance, agriculture, education, and economic growth.

© DAI Global, LLC

The opinions expressed are those of the authors and do not necessarily represent the views of any government or donor agency associated with the content of this paper.

Cover Photo: UN Women/Gaganjit Singh

Design: Jennifer Geib

CONTENTS

EXECUTIVE SUMMARY	4
INTRODUCTION	7
DIGITAL INCLUSION AND A TRUSTED INTERNET	13
RECOMMENDATIONS	15
CONCLUSION	20
REFERENCES	21
ACKNOWLEDGEMENTS	22

EXECUTIVE SUMMARY

The international development community has embraced the potential of digital technology to expand the reach of life-enhancing services and provide a platform for collaboration and innovation. For at least the past two decades, international development practitioners have turned to digital tools to improve the delivery of traditional development programs in health, education, agriculture, and so on. More recently, digital inclusion—that is, direct efforts to extend internet access to previously unserved populations and accelerate the adoption of digital services—has emerged as an international development practice in its own right.

In many instances, development programs have realized the promise of digital technology: mobile phones are reducing infant mortality rates by delivering critical health information to new mothers, internet access is enabling small businesses to reach global markets, and digital identity programs are facilitating access to legal and financial services for refugees.

There is, however, an increasingly strong countervailing force to such progress: the erosion of trust in the internet driven by an accelerated spread of misinformation, new forms of government surveillance, and the exponential growth of cybercrime.

Such unintended consequences of the rapid proliferation of digital technology have thrust into the spotlight the role of the development community in expanding internet access in emerging markets. In particular, these challenges have highlighted the inherent tensions between digital access and cybersecurity. As a report commissioned by Microsoft's Trustworthy Computing Group explained,

“A completely secure computer or network is one with no connections to external sources, but this renders it almost futile for most modern applications. Yet as the number of access points in a society increases, so do the vectors for an opportunistic attacker to travel. Expansion of access multiplies the number of potential vulnerabilities....Therefore neither absolute safety nor absolute convenience is attainable or desirable.”¹

On one hand, nearly half the world's population remains offline—a status quo that should be unacceptable to development practitioners concerned with supporting economic growth, social inclusion, and new opportunities for historically marginalized populations. On the other hand, low-income countries where most offline populations are found are the least prepared to respond to cyber threats,² potentially putting at greater risk the very populations that internet access programs seek to connect. Given the international development community's role in shaping the digital ecosystem in emerging markets, it must seek to encourage the right balance between access and security.

Drawing on both the author's experience as well as a small but growing body of literature on the interplay of cybersecurity and international development, this report offers international development donors, particularly bilateral donors, recommendations for navigating the trade-offs implicit in the access-security debate.

The report looks at the current context and emerging trends that have increased the urgency for development donors to refine their approach to the relationship between access and security. It then focuses on digital

inclusion programs specifically, arguing that, if countries are to effectively navigate the relationship, they should resist calls to mainstream cybersecurity and instead take a more targeted approach to building a trusted digital space. In particular, the paper looks at three key areas where international donors have a unique role to play:

- 1 Empowering users to be dynamic participants in the digital space
- 2 Supporting governments' capacity to develop and implement integrated national digital strategies
- 3 De-risking digital inclusion investment in emerging markets to catalyze innovation, spur competition, and build an ecosystem of trusted partners

Within each of these areas, the report offers concrete recommendations on what can be done in the next two to three years. Some of the recommendations build on existing literature while others are new and intended to provoke further discussion among development practitioners and between the development and cybersecurity communities.



The rapid proliferation of digital technology has highlighted the inherent tensions between digital access and cybersecurity.



Given the persistent digital divide, donors supporting digital inclusion should prioritize investments to expand an access environment that cultivates trust among internet users, service providers, and governments. In doing so, they will help preserve the internet as an engine of inclusion and social benefit for poor and marginalized populations.

INTRODUCTION



In 2014, the U.S. Department of State Cyber Coordinator's Office held the first in a series of trainings designed to equip foreign service officers with the knowledge and tools needed to represent the policy priorities enumerated in the President's International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.

The training's first session, on the power of internet access to drive economic growth, was followed immediately by one on cybercrime, delivered by a high-ranking military officer who drew on recent headline-making cyber attacks—such as the 2012–2013 Operation Ababil, which targeted U.S. financial institutions with distributed-denial-of-service attacks—to paint a dire picture of escalating risks in the virtual world. That presentation was followed by others on cyber warfare, online fraud, the use of online platforms for state-sponsored surveillance, and other nefarious aspects of the digital age. By the end of the training, it was clear that the message of digital “risk” resonated with participants far more than the message of digital “opportunity.” At best, the policies for promoting digital access and the policies for preventing cyber risk appeared as disconnected issues and, at worst, as fundamentally at odds.

From a practitioner perspective, the tension evident at this training reflects a broader reality: two generally distinct fields of practice. When questions about the access-security relationship surface in digital inclusion programs, the

common answer has been, in principle, self-evident: efforts to expand access to or adoption of digital technology should mean supporting secure and reliable access. In practice, however, implementing programs that balance internet access and cybersecurity is more complex. In addition to practical considerations such as budget trade-offs, there are more fundamental questions about the inherent value of a free and open internet and the extent of a government or a company's responsibility to mediate how individuals experience the internet.

As these questions bring together diverse stakeholders from across sectors and from different parts of government—including defense, intelligence, diplomatic, and development agencies—bilateral development donors may be tempted to adopt a more risk-averse position that favors securing networks over expanding access, much as the threat of risk had more traction than the message of opportunity at the 2014 State Department training.

Given the persistent digital divide, donors supporting digital inclusion efforts must resist this temptation. Instead, they should prioritize investments to expand an access environment that cultivates trust among internet users, service providers, and governments. In doing so, they will help preserve the internet as an engine of inclusion and social benefit for poor and marginalized populations.

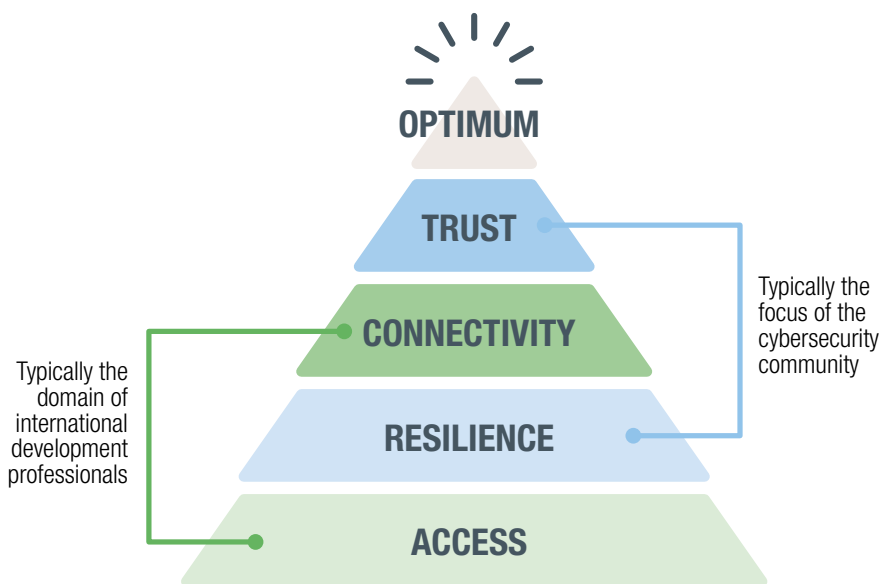
Background

Questions about the relationship between information and communication technology (ICT)-driven development and cybersecurity are not new. In 2011, the United Nations Economic and Social Council (ECOSOC) convened an event to provide members with a global view on emerging policy recommendations for cybersecurity and how those recommendations related to national development policies.³ In 2013, Microsoft released its *Hierarchy of Cybersecurity Needs: Developing National Priorities in a Connected World*, which borrowed from Maslow's hierarchy of human needs to suggest how countries can maximize the benefits of the internet by aligning cybersecurity priorities with citizen needs.⁴

Both efforts told the same story: digital technology had become an indispensable component of social and economic development, underpinning an increasing number of products and services and cutting across sectors, but the risks to the digital ecosystem were expanding. These risks had the potential to erode trust in tech-enabled systems, reduce their resilience, and undermine their potential to effect positive social and economic change. The Hierarchy of Cybersecurity Needs argued that in an optimally used internet (equivalent to Maslow's self-actualization), the opportunities and risks are inherently linked. In-

dividuals first need access to the internet, the networks then need to be reliable and resilient, then individuals need to be able to use said networks to connect with other people and with services, and lastly the entire system needs to promote trust—between individuals, between individuals and service providers, between individuals and governments, between governments and private actors, and between governments.⁵

Notwithstanding this emerging understanding, international development and cybersecurity efforts have remained largely separate, supported by distinct stakeholders and implemented with distinct strategies and budgets. In many respects, the first (access) and the third (connection to people and services) levels of the Hierarchy have been the domain of international development professionals, while the cybersecurity community has focused more on the second (resilience) and fourth (trust). Of course, these are complex issues with inevitable overlap (ensuring personal data security in a mobile health program, for example), but this framing is useful for understanding where efforts have focused and where there are opportunities for better collaboration and decision making.



Hierarchy of Cybersecurity Needs

Microsoft's Hierarchy of Cybersecurity Needs

In an effort to help guide the development of national cybersecurity policies, in 2013 Microsoft suggested how countries can maximize cybersecurity priorities with the citizen needs. (graphic adapted from *Hierarchy of Cybersecurity Needs: Developing National Priorities in a Connected World*).



Cybercrime is eroding users' trust in the digital space which, in many respects, will be far harder to recoup than any monetary losses, particularly in emerging markets as new users come online for the first time.

Relevant Trends

A renewed push for a more cohesive approach to cybersecurity and development was catalyzed by the World Bank's World Development Report 2016, which noted "some of the perceived benefits of digital technologies are offset by emerging risks."⁶ And in 2018, New America released *Securing Digital Dividends*, which makes the case specifically for mainstreaming cybersecurity across international development,⁷ much as gender mainstreaming has been formalized as an approach for achieving gender equality and women's empowerment at all levels of development. This push is a response to two trends:



The development community's embrace of digital technology

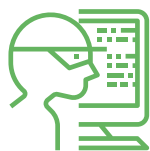
By the end of 2018, there will be more than 4 billion internet users, an increase of more than a billion in the past couple of years. This growth has been driven by increasingly affordable smartphone and data plans as well as innovations in broadband access technologies. Importantly, regions where internet usage has lagged historically are now seeing some of the fastest growth. Africa, for instance, is experiencing 20 percent year-on-year growth; countries such as Benin, Mozambique, Niger, and Sierra Leone have doubled internet usage in the past year.⁸ This continued expansion of the internet means that more than half the world is now online, and the use of ICTs across traditional development sectors like health, education, and financial inclusion has only grown in importance and scale. By 2015, the World Summit on the Information Society was calling

on all "governments, the private sector, civil society, international organisations, the technical and academic communities and all other relevant stakeholders to integrate information and communication technologies in their implementation approaches to the SDGs."⁹ In 2017, the World Bank estimated that 80 percent of its projects have an ICT component.¹⁰

The development community has not only embraced technology as an enabler of development outcomes but also started to invest in building a stronger foundation for the digital ecosystem. Universal access to the internet has, in its own right, become the focus of international efforts—such as the World Economic Forum's Internet for All project—and enshrined in the Sustainable Development Goals (SDGs).



SDG 9.C: 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.

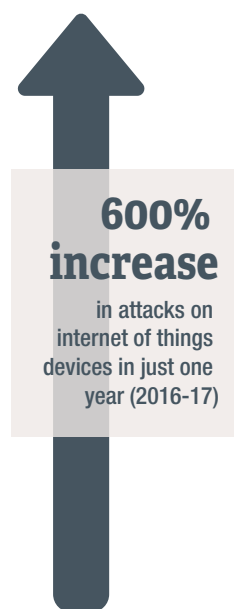


The exponential increase in cybercrime and the erosion of trust

By 2016, cybercrime was the second most reported crime globally.¹¹ In the same year, it accounted for more than 50 percent of crime in the United Kingdom.¹² Between 2013 and 2015, cases of fraud using mobile channels increased by 173 percent globally,¹³ and between 2016 and 2017 attacks on internet-of-things devices increased 600 percent.¹⁴ A litany of high-profile public security breaches—from Equifax to Facebook-Cambridge Analytica—has exposed the personal data of hundreds of millions of people.

This trend shows no sign of abating and promises to be a drag on the global economy, with some estimates suggesting cybercrime will cost the world \$6 trillion annually by 2021—twice what it cost in 2015 and more profitable than the global trade of all illicit drugs combined.¹⁶

Cybercrime is eroding users' trust in the digital space which, in many respects, will be far harder to recoup than any monetary losses, particularly in emerging markets as new users come online for the first time. The 2018 CIGI-Ipsos Global Survey on Internet Security and Trust found that 52 percent of internet users surveyed around the world are more concerned about their online privacy than they were a year ago, and this diminishing trust is beginning to influence user behavior: 12 percent of those surveyed are using the internet less to make purchases and 7 percent are using the internet less often overall, compared to a year ago.¹⁷ In a similar 2017 survey in the United States, 45 percent of respondents said they had changed their behavior online based on their fears.¹⁸



Cyberattacks will cost the world

\$6 trillion
annually by 2021

Exponential Growth of Cyber Attacks

(Adapted from Internet of Things).¹⁵

Time for Action

In response to these trends, a handful of developed countries have developed whole-of-government digital strategies to address the relationships between technology-driven growth, cybersecurity, data privacy, and civic participation. Additionally, large bilateral donors, including the United States and United Kingdom, are linking investments in expanded internet access in emerging markets and investments in cybersecurity.

Furthermore, security breaches in developed nations have prompted a backlash against the technology community, with both the public and governments demanding more transparency and accountability from the tech sector. Given this, general trust of the internet remains higher in emerging markets than it does in more developed countries, with 21 percent of respondents from the Middle East and Africa strongly agreeing with the statement, “Overall, I trust the Internet,”¹⁹ compared to only 9 percent of respondents from G8 countries.

The development community has a responsibility to strengthen the culture of trust around the internet in emerging markets before the backlash seen in developed markets takes root globally and becomes a barrier to new users coming online and to responsible deployment of digital tools in development programs. The next two to three years will be a critical period for the development community to develop a clear approach to integrating trust into digital inclusion programs.

We do not know where the optimal equilibrium between digital access and security lies—all countries are still learning how to navigate the difficult trade-offs and there will always be some level of calibration needed. And the international development community should not be looking to implement a single, prescriptive model for balancing access and security. Rather, it should use the expansion of trusted access as a guidepost while helping to strengthen countries’ ability to assess and respond to their own context.



The development community has a responsibility to strengthen the culture of trust around the internet in emerging markets before the backlash seen in developed markets takes root globally and becomes a barrier to new users coming online and to responsible deployment of digital tools in development programs.

DIGITAL INCLUSION AND A TRUSTED INTERNET

Why Emphasize Trust?

A recent survey of academic literature identified some 200 different definitions of the term “cybersecurity.” As Microsoft noted in a 2014 report, “[Cybersecurity] takes on different meanings depending on the audience. Citizens may feel that cybersecurity is related to protecting personal information, while businesses may view it as a means for providing business continuity. In the policy context, cybersecurity represents the collective activities and resources that enable citizens, enterprises, and governments to meet their online objectives in a secure, private, and reliable manner.²⁰” This paper does not try to navigate these definitional complexities, nor should that be the role of international development donors or practitioners. However, this definitional diversity highlights two important points: 1) the cybersecurity community views its work as far more than avoidance of cyber threats, and 2) calls to mainstream cybersecurity into development need to be unpacked in order to design and implement good programs. Protecting privacy and protecting critical network infrastructure, for instance, are both cybersecurity priorities, but programs to address them would be distinct.

In October 2017, New America convened cybersecurity and development professionals to discuss ways to expand collaboration between the two communities. The breakthrough in the discussion came when one cybersecurity expert noted that collectively the two communities need to start talking about “security for” instead of “security from.” Seen in this light,

cybersecurity is more than simply a defensive posture that would most naturally fit within the mandate of the defense and intelligence communities. As Sandra Sargent from the World Bank’s Transport and ICT Global Practice puts it, cybersecurity is about the economy, good governance, banks, hospitals, companies, banks, citizens, and so on.²¹


This framing is a first step in better calibrating the access-security relationship by aligning goals and creating a common vocabulary between development and security advocates. It encourages the development community to think of the security of digital spaces as an enabler of positive development outcomes.

Donors are well positioned to facilitate strategic collaboration between the two communities and can do so by asking three key questions:

- ❓ Where is there strong alignment between cybersecurity and development outcomes?
- ❓ Where do development donors and practitioners have a comparative advantage over traditional security organizations in strengthening cybersecurity?
- ❓ Where is there persistent underinvestment in building a more secure digital ecosystem?



Framing the discussion around “security for” rather than “security from” is a first step toward aligning the goals and vision of the development and security advocates.



By integrating trust more intentionally into digital inclusion programs, the development community can continue to pursue its poverty alleviation and social inclusion goals while contributing to the broader security environment in a targeted way.

Introducing Trust into Digital Inclusion

The development community's increasing reliance on digital tools and services to deliver programs requires that individuals trust the digital space enough to use them, squarely aligning development goals with the need to invest more in building trust. In 2017, the Internet Society released its policy framework for an open and trusted internet, largely in response to the erosion of trust described above. The paper offered the following definition of the trusted internet:

"A 'trusted Internet' is a globally, distributed, interoperable network of networks that cultivates innovation and creates opportunities for all.... There will always be risks and downsides to an open network system.... Technologies and capabilities we develop to improve one part of life may negatively impact another. But, threats can be mitigated, risks distributed, weaknesses shared and repaired."²²

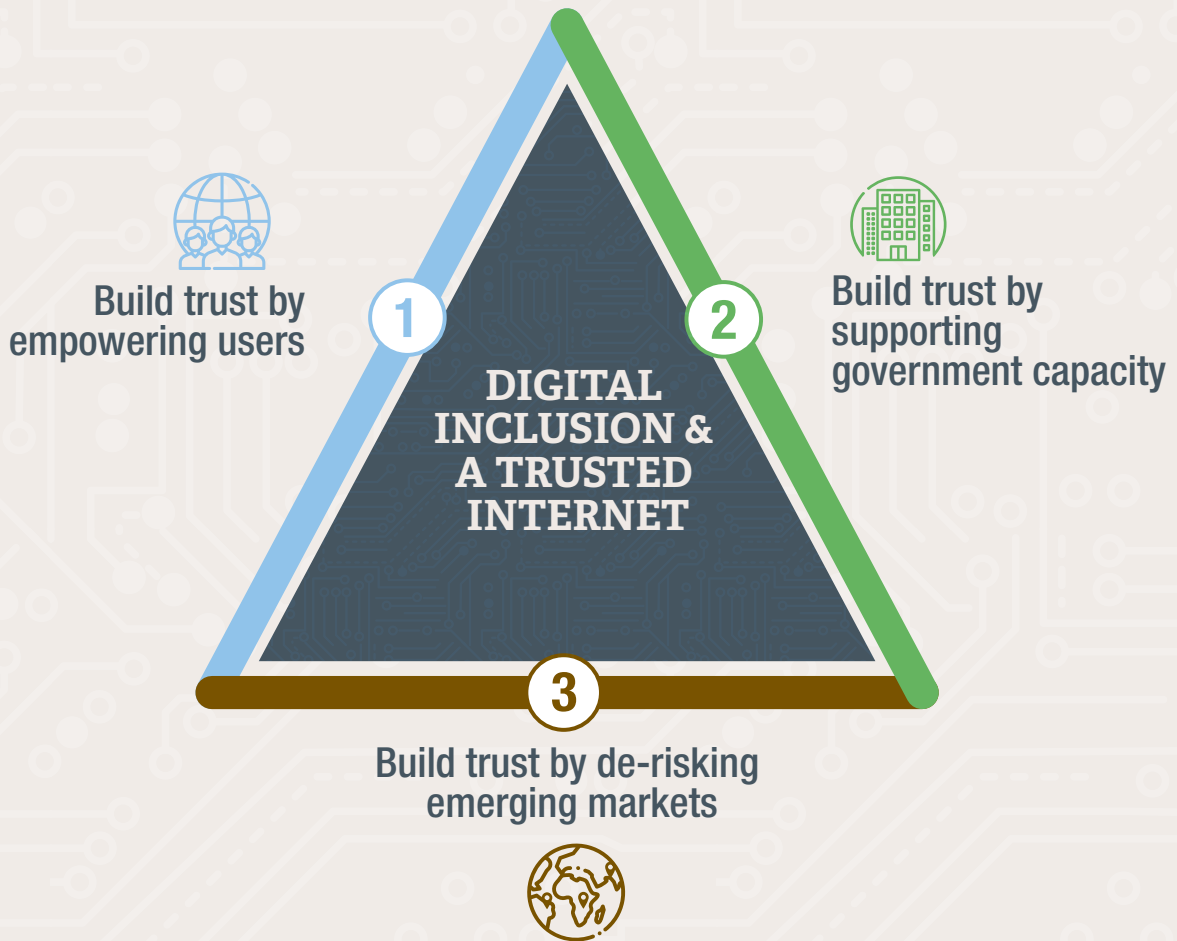
The paper focused on the role of government in creating a policy environment conducive to realizing this vision but emphasized the need for a collective approach. The international development community must play a more active role in this collaborative effort and already has tools and models available to do so.

The initiatives that have emerged over the past five years to advance digital inclusion have all focused on some combination of expanding physical access to the internet, making access more affordable, supporting digital literacy, building user awareness of the internet and its benefits, and cultivating local content ecosystems.* These essential attributes of an open and inclusive digital space should remain focal points for digital inclusion investments, complemented—not replaced—by the promotion of trust. By integrating trust more intentionally into digital inclusion programs, the development community can continue to pursue its poverty alleviation and social inclusion goals while contributing to the broader security environment in a targeted way.

* It is important to acknowledge that the international development community already does address trust in digital programs in some meaningful ways. The Principles for Digital Development, for instance, include among nine core tenets a clear commitment to privacy and security of data, noting "Following data privacy practices and security safeguards protects the interests of communities, while promoting trust between end users and digital development practitioners." The U.S. Agency for International Development's paper, *Identity in the Digital Age*, likewise takes a close look at the ways in which digital identity can cultivate trust.

RECOMMENDATIONS

The following recommendations for integrating trust into digital inclusion programs are intended to add to the various ways the development community cultivates trust, not replace them.





Recommendation 1: Build Trust by Empowering Users

Individual internet users are becoming passive recipients of information and commerce online. For most internet users coming online today, the origins of the internet as a platform for collaboration and innovation have been lost and the passive nature of their online experience has limited individuals' sense of empowerment. This lack of agency erodes trust, particularly in an environment where misinformation and cybercrime are growing. A 2018 Reuters survey found that more than half of all internet users are concerned about the authenticity of news online, and 70 percent felt it was the responsibility of content publishers and platform companies to fix this problem.²³ These actors certainly have a role to play, but digital inclusion programs in emerging markets can also cultivate a more trusted digital ecosystem by helping individuals regain a sense of agency over their activities online.

Many experts believe that dwindling trust will not be a barrier to increased public reliance on the internet because its sheer convenience will lead people to use online products and services despite their misgivings.²⁴ From a development perspective, these projections are troubling. If digital inclusion programs do not also address trust in the networked environment they are helping to create, they risk constraining or even reversing the intended benefits of expanded access—creating channels for government control, online fraud, and the incitement of hatred and division.

Recommendations to Donors



Donors can support efforts to build trust in the internet by empowering users through policy efforts and through direct engagement with individuals.



Donors should promote policies and regulations that guarantee individuals' privacy and freedom from pervasive surveillance, regardless of nationality or residence, and give individuals greater agency over the personal data that they generate online and that is collected about them.²⁵



Donors can cultivate user empowerment in several ways. In any program that involves the use of digital tools or services, they should insist on adherence to the Principles for Digital Development and explain those principles to program participants. Digital inclusion programs can leverage existing efforts to increase digital literacy as a channel through which to build trust. Digital literacy training, often part of digital inclusion programs, is a natural opportunity to integrate cybersecurity priorities, perhaps by exploring issues such as consumer rights, identity and confidentiality, and privacy and security.



Internet users will have a clearer understanding of their privacy and consumer rights, greater ability to assess online risks and identify misinformation and efforts to manipulate, and more agency in their lives online.



Recommendation 2: Build Trust by Supporting Government Capacity

While significant progress has been made to integrate digital policy into national development strategies, most governments have yet to create cohesive policies or unified technology architectures across line ministries. Additionally, efforts to develop digitization strategies have typically been independent from national cybersecurity planning. Furthermore, only 38 percent of the International Telecommunication Union's members have a cybersecurity strategy and only 21 percent publish any metrics on cybersecurity incidents in their countries,²⁶ making it difficult for governments to plan for, identify, understand, and respond to risks. This fragmentation often results in disjointed or delayed responses to digital risks, thereby diminishing overall trust in the system.

Even in the face of increasing cyber risks globally, governments can cultivate a more trusted digital space by establishing clear strategies, practicing transparent decision making, and demonstrating the capacity to implement national plans. Estonia's experience, often cited as a model, is informative. Following cyber attacks on the nation's banks, media outlets, government bodies, and general populace in 2007, Estonia's government led a coordinated response: temporarily shutting down internet service, addressing vulnerabilities, and forthrightly communicating to citizens what had happened and what it planned to do about it. In contrast to governments that either suppress news of vulnerabilities or lack the capacity to track cyber attacks, Estonia's government is now seen as committed to keeping its people and their information secure online.

Recommendations to Donors

The Internet Society's trust framework provides governments with detailed policy recommendations. The following recommendations highlight two steps international development donors should take to reinforce the vision laid out by the Internet Society.



Work with the cybersecurity community to develop a digital capacity building program that addresses the balance between access and security. The cybersecurity community has emphasized building government capacity to identify, assess, and respond to threats. Meanwhile, the international development community is working in parallel to achieve universal internet access. Efforts to engage the cybersecurity community on a standard digital capacity building program will enable the development community to represent its interests in an open and inclusive internet, while working together to put in place safeguards that can help build trust.



Support the development of national digital strategies created and owned by governments. Too often, governments outsource the preparation of digital or cybersecurity strategies, and too often this leads to a lack of country ownership, regardless of the internal capacity to implement them. Donors should support participatory and inclusive processes for developing digital strategy. Donors can fund subject matter experts to advise governments and might facilitate learning from other countries and global organizations, but they should ensure that partner governments undertake a participatory and inclusive process that brings in local development and cyber representatives, line ministries, and other local stakeholders.



National governments will have a clearer stake in decision making and will be better able to balance access and security based on local needs. By focusing on standardization of capacity-building programs and local ownership, the development community can help establish parameters that underpin a free and open internet while building a more trusted digital ecosystem that responds to local context.



Recommendation 3: Build Trust by De-Risking Emerging Markets

Increasingly, emerging market governments are turning to state-controlled companies that offer subsidized loans to build out broadband networks. This reliance on state-sponsored companies and their equipment has led to an erosion of trust in emerging markets, driven by both real and perceived threats. For instance, reports emerged earlier this year that China, which paid for and built the African Union (AU) headquarters' computer network, had inserted a backdoor into the system that affords access to confidential information on AU servers.²⁷

It is understandable why emerging market governments turn to such companies. Chinese firms, for example, are often competitive on cost, and alternatives sometimes don't exist. As Steve Song, the founder of Village Telco, notes in a report on African telecom infrastructure: "The development of terrestrial fibre optic infrastructure on the [African] continent continues apace with the Chinese government, the World Bank and the African Development Bank leading as the principal financiers of these networks. Huawei continues to dominate the terrestrial fibre business in Africa. No other name is seen remotely as often as theirs linked to the construction of a terrestrial fibre network on the continent."²⁸ Meanwhile, most fully commercial entities view emerging markets as inherently risky, compounding the problem and reducing the number of trusted partners.

Recommendations to Donors

Donors already have the tools to incentivize new market entrants, but such measures have been used too infrequently to support the expansion of internet access infrastructure. These donor tools fall into three primary categories:

Direct co-financing of infrastructure to assume some risk in markets private actors would otherwise avoid

Creative solutions for unlocking commercial financing through loan guarantees and other risk-sharing facilities


Capacity building to support stronger and more independent regulatory bodies, and policy levers to promote more open and competitive markets

Indeed, we see an increasingly rich array of channels through which international donors can unlock private capital in support of the first two categories. Risk-sharing and loan guarantee facilities, such as USAID's Development Credit Authority, can unlock commercial investment in risky markets. Donor governments are creating and strengthening government-owned or government-managed development finance institutions. In the United Kingdom, the CDC Group has growing influence in implementing the country's development priorities, a mandate to make riskier investments, and a growing budget.²⁹ Similarly, the passage of the Better Utilization of Investments Leading to Development (BUILD) Act in the United States is likely to greatly expand the U.S. Government's support for development finance.³⁰ These institutions and the various investment mechanisms they can support represent a tremendous opportunity to create a more dynamic and competitive telecom sector in emerging markets, thereby expanding the universe of potential trusted partners.

The creation of these investment vehicles, however, is only a first step. The development community still has a significant role to play in realizing this potential.

 **Donors investing in digital inclusion must be vocal in making the case to investment institutions that digital inclusion is essential to social and economic development.** Thirty years ago the development sector saw digital technologies like mobile phones as luxury items, leading institutions like the International Finance Corporation (IFC) to decide, for instance, that investing in mobile network operators was beyond its mandate. At IFC, that view changed in the 1990s, and the development community has now embraced digital technology. That said, two factors inhibit more active development sector investment in digital inclusion: first, the perception that the private sector will take care of internet access; second, the fact that while investments in the use of technology have increased dramatically, investment in the more foundational elements of digital development—such as broadband access—have been inconsistent. Digital inclusion programs must make the case to development finance institutions that they are uniquely positioned to expand the reach of commercial telecom and that this foundational investment will be a platform upon which other development programs can build.

 **Donor support for creating standardized digital risk assessments will help potential investors understand and assess their risks.** In *Securing Digital Dividends*, New America called for the creation and implementation of such a tool, suggesting it follow a similar model to environmental and human rights impact assessments.³¹ This kind of standardized risk assessment tool would be extremely useful if deployed in all digital inclusion programs as well as programs using digital tools to support better outcomes in traditional development sectors.

 **Large-scale financing efforts for broadband access often select vendors primarily based on cost.** In the worst situations, political interests also factor into the way that broadband efforts are designed around the narrow economic interests of the incumbent provider. Vendor selection processes rarely take into account network security. The international development community should support a multi-stakeholder group—which may include multilateral development banks, other donors, and governments—to convert existing principles on affordable access, network security, privacy, and other relevant topics into a common set of actionable and enforceable standards that set basic parameters for a trusted network while enabling customization based on local needs.



Paired with strong due diligence processes and procurement standards, these de-risking tools will encourage additional market entrants, thereby expanding the potential universe of trusted partners and offering internet users—individuals, enterprises, and governments—more choice in their service providers. Efforts to de-risk investment will also allow for expanded innovation in business models and last-mile technology solutions. Donors can ensure that the innovations they support use available digital risk assessment tools and meet standard due diligence requirements, thereby further supporting the growth of a trusted digital ecosystem.



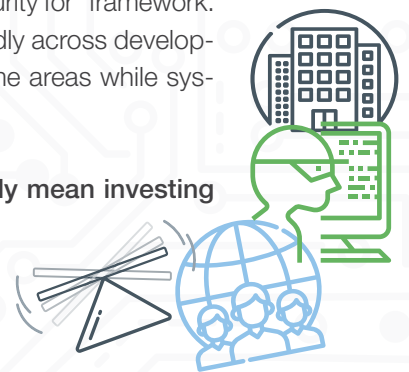
CONCLUSION

Donors have an opportunity to play a formative role in the future direction of the internet. The increasing risks online—both real and perceived—are often cited to justify a more centrally controlled and closed internet. Conversely, the internet’s potential to drive positive socioeconomic change, especially when seen against the backdrop of a persistent digital divide, is cited as a reason for supporting universal access.

Ultimately, the development goals of inclusive economic growth and expanded access to information are best served by an open and inclusive internet. Achieving this vision should remain the objective of the development community, but it must take seriously the risks presented by expanded access. Getting the cybersecurity environment right will require collaboration among different communities—law enforcement, defense, intelligence, diplomatic, and others. But the development community should exert its interests and resist pressure to adopt a risk-averse position that prioritizes security over inclusion. The “security from” construct is important but remains the domain of other actors.

International development donors should find ways to advance the “security for” framework. Doing so, however, does not mean mainstreaming cybersecurity broadly across development programs. Instead, donors should facilitate collaboration in some areas while systematically integrating trust into digital inclusion programs.

Moving forward, investing in “internet access” should necessarily mean investing in “trusted internet access.”



REFERENCES

- 1 Oxford Analytica, Commissioned by Microsoft Trustworthy Computing (2013, November). *Hierarchy of Cybersecurity Needs: Developing National Priorities in a Connected World*. Retrieved from <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVMca>
- 2 International Telecommunications Union (2017). *Global Cybersecurity Index 2017*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GC\I.01-2017-R1-PDF-E.pdf
- 3 United Nations Economic and Social Council (2011). *Issues Notes: Special Event on Cybersecurity and Development*. Retrieved from http://www.un.org/en/ecosoc/cybersecurity/concept_note.pdf
- 4 Oxford Analytica (2013). *Hierarchy of Cybersecurity Needs*.
- 5 Oxford Analytica (2013). *Hierarchy of Cybersecurity Needs*.
- 6 World Bank. 2016. *World Development Report 2016: Digital Dividends*. Washington, DC: World Bank. doi:10.1596/978-1-4648-0671-1. License: Creative Commons Attribution CC BY 3.0 IGO.
- 7 Morgus, Robert (2018, April 23). *Securing Digital Dividends: Mainstreaming Cybersecurity in International Development*. New America. Retrieved from https://s3.amazonaws.com/newamerica-dotorg/documents/Securing_Digital_Dividends_Gv2FUiZ.pdf
- 8 Kemp, Simon. (2018, January 30). Digital in 2018: World's Internet Users Pass the 4 billion mark. Retrieved from <https://wearesocial.com/blog/2018/01/global-digital-report-2018>
- 9 Niels Nagelhus Schia (2018) *The cyber frontier and digital pitfalls in the Global South*, Third World Quarterly, 39:5,821-837, DOI: 10.1080/01436597.2017.1408403. Retrieved from <https://www.tandfonline.com/doi/full/10.1080/01436597.2017.1408403>
- 10 Sargent, Sandra (2017). *World Bank Donor Perspective on Cybersecurity*. World Bank, Transport and ICT Global Practice. Retrieved from <http://www.cto.int/media/events/pst-ev/2017/cybersecurity%202017/Sandra%20Sargent%20The%20World%20Bank.pdf>
- 11 PricewaterhouseCoopers (2018). *Pulling Fraud out of the Shadows: Global Economic Crime and Fraud Survey 2018*. Retrieved from <https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html>
- 12 National Crime Agency Strategic Cyber Industry Group (2016, July 7). *Cyber Crime Assessment 2016 Need for a stronger law enforcement and business partnership to fight cyber crime*. Retrieved from <http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file>
- 13 RSA (2016). 2016: Current State of Cybercrime. Retrieved from <https://www.rsa.com/content/dam/premium/en/white-paper/2016-current-state-of-cybercrime.pdf>
- 14 http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq
- 15 Symantec (2018, March). *Internet Security Threat Report*. Retrieved from: http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq
- 16 Cybersecurity Ventures (2017, October 16). *Cybercrime Damages \$6 Trillion By 2021*. Retrieved from <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- 17 Center for International Governance Innovation and Ipsos (2018). *2018 CIGI-Ipsos Global Survey on Internet Security and Trust*. Retrieved from <https://www.cigionline.org/internet-survey-2018>
- 18 Internet Society (March 2017). *A Policy Framework for an Open and Trusted Internet: An approach for reinforcing trust in an open environment*. Retrieved from <https://www.internetsociety.org/wp-content/uploads/2017/08/bp-Trust-20170314-en.pdf>
- 19 Center for International Governance Innovation and Ipsos (2018). *2018 CIGI-Ipsos Global Survey on Internet Security and Trust*.
- 20 Burt, David, Nicholas, Paul, and Sullivan, Kevin (Microsoft Trustworthy Computing) and Scoles, Travis (Schireson Associates) (2014). *The Cybersecurity Risk Paradox: Impact of Social, Economic, and Technological Factors on Rates of Malware*. Microsoft Corporation. Retrieved from <https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-risk-paradox>
- 21 Sargent (2017). *World Bank Donor Perspective on Cybersecurity*.
- 22 Internet Society (March 2017). *A Policy Framework for an Open and Trusted Internet*.
- 23 Newman, Nic with Fletcher, Richard, Kalogeropoulos, Antonis, Levy, David A. L., and Nielsen, Rasmus Kleis (2018). *Digital News Report 2018*. Reuters Institute and University of Oxford. Retrieved from <https://agency.reuters.com/content/dam/openweb/documents/pdf/news-agency/report/dnr-18.pdf>
- 24 Raine, Lee and Anderson, Janna (2017, August 10). *The Fate of Online Trust in the Next Decade*. Pew Research Center: Internet & Technology. Retrieved from <http://www.pewinternet.org/2017/08/10/the-fate-of-online-trust-in-the-next-decade/>
- 25 Internet Society (March 2017). *A Policy Framework for an Open and Trusted Internet*.
- 26 International Telecommunications Union (2017). *Global Cybersecurity Index 2017*.
- 27 Dahir, Abdi Latif (2018, January 30). *China "gifted" the African Union a headquarters building and then allegedly bugged it for state secrets*. Quartz Africa. Retrieved from <https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/>
- 28 Song, Steve (2018, January). *Africa Telecoms Infrastructure in 2017*. Retrieved from <https://manypossibilities.net/2018/01/africa-telecoms-infrastructure-in-2017/>
- 29 Anders, Molly (October 2017). *CDC kicks off new strategy with eye toward riskier investments*. DevEx. Retrieved from <https://www.devex.com/news/cdc-kicks-off-new-strategy-with-eye-toward-riskier-investments-91328>
- 30 Ingram, George (2018, July 10). *How the BUILD Act Advances Development*. Brookings. Retrieved from <https://www.brookings.edu/blog/future-development/2018/07/10/how-the-build-act-advances-development>
- 31 Morgus (2018). *Securing Digital Dividends*.

ACKNOWLEDGEMENTS

This report would not have been possible without the institutional and financial support of DAI's Center for Digital Acceleration. The author wishes to express his gratitude to DAI's Krista Baptista for conceiving the project and for her guidance and advice throughout. Thanks also to DAI's Steven O'Connor, Kurt Olsson, Kristen Roggemann, Anand Varghese, and the rest of the CDA team for their careful review, substantive input, and editing of various drafts as well as their dedication to the project. Finally, the author wishes to express his appreciation for the many colleagues and friends who offered formal and informal feedback—you know who you are and your support has been invaluable.



DAI Center for Digital Acceleration

digital@dai.com | <https://dai-global-digital.com/>