Securing the Modern Economy:

Transforming Cybersecurity Through Sustainability

by Megan Stifel

April 2018

Public Knowledge

Executive Summary

Headlines remind us daily that our use of technology is fraught with opportunity and risk. The advent of the internet and other information and communications technologies has fostered economic growth, modernized industry, and simplified daily life. At the same time, consumers feel less secure in their engagements online, which is contributing to a growing distrust of technology. Cybersecurity, or information security, are efforts undertaken to ensure the confidentiality, integrity, and availability of information. Considered broadly, cybersecurity includes a range of societal policies, from education and consumer awareness to insurance programs, corporate governance, and international relations. Maintaining public trust in technology relies in significant part on all stakeholders prioritizing cybersecurity.

Weak device security and constrained network management practices recently enabled a distributed denial-of-service (DDoS) attack to knock out portions of the internet on the U.S. East Coast. In 2016, organizations' fraud loses increased over 60 as a result of consumer account takeovers facilitated by password compromises.[1] These outages and loses demonstrate that the current cybersecurity compliance and risk management models allow for too much short-term focus that has not and can not build the types of resilient technologies necessary to support long-term public confidence and sustain the economic growth that development and adoption of interconnected things, also known as the "Internet of Things," or IoT, can foster. Known insecurities together with thousands more devices forming the Internet of Things create a ticking time bomb that risks a calamity of public confidence that could undermine the modern economy and democratic institutions. If we want to avoid this public trust disaster, we must adopt a sustainable approach to cybersecurity.

Governments, industry, and civil society generally agree that the internet and information and communications technologies (ICTs) are a shared resource and a unique ecosystem. They also increasingly recognize that cybersecurity is a common good. As such, in addition to a cybersecurity moonshot to improve the security of the internet ecosystem, we must also look to effective societal approaches that employ common goods to successfully manage ecosystems. Sustainability is one such successful approach. Sustainable cybersecurity is an approach in which stakeholders' interactions with the ICT ecosystem are understood and deliberate, and where each participant understands its responsibility as a steward to respect and protect the ecosystem to preserve its future use.

While all analogies ultimately break down, elements of sustainability management are particularly relevant to cybersecurity. To begin, companies that adopt sustainability governance practices are more successful than those that do not. Thus, contrary to the common perception that "doing good" cuts in to "doing well," adopting sustainable policies can add to an organization's bottom line. This is also the case for implementing cybersecurity best practices. Moreover, ICTs underpin almost every modern-day

[1] RSA Ebook, *2017 Consumer Cybersecurity Confidence Index*, at 2 (last visited April 12, 2018), https://www.rsa.com/content/dam/pdfs/5-2017/rsa-consumerconfidenceindex-ebook.pdf.

transaction, from the delivery of electricity and water to banking, shopping, manufacturing, and correspondence. As is increasingly apparent, failure to ensure the confidentiality, integrity, authenticity, or availability of the information facilitating these activities can result in critical failures for associated and unrelated information, devices, and actions. These failures risk reputation, income, assets, and the very longevity of the organization as a going concern. As a result, like sustainability, cybersecurity is becoming a "C-suite" issue. Just as past business operations may have contributed to climate change and other traditional sustainability challenges, many of today's cybersecurity issues are the result of business practices that failed to adequately consider the broader implications of a particular decision.

The sustainability movement and cybersecurity also have in common the opportunities and challenges of interoperability and scale. Sustainability policy emerged from the need for global collective action. In recent decades, large groups of stakeholders across the world have adopted sustainability policies and programs to tremendous effect. Similarly, ICT interoperability has fostered an ever-expanding global marketplace and strong economic growth. But that marketplace and associated growth are at risk from growing distrust of ICTs due in part to their inadequate security. Sustaining cybersecurity in the modern economy means being intentional about interoperability and the business choices that should be made to securely enable it.

Noteworthy, too, is the critical role cybersecurity plays in core sustainability practices. As with most operations today, information and communications technologies increasingly, if not completely, support traditional sustainability actions as identified by the United Nations Global Compact 10 Principles and the 17 Sustainable Development Goals. In addition to operational tracking and compliance to achieve desired objectives, these sustainability policies and processes also enable organizations to be more transparent about their decisions. Furthermore, the cybersecurity nexus to these now commonplace business practices suggests organizations' existing sustainability processes and policies likely provide a foundation upon which to incorporate and scale enhanced approaches to cybersecurity, including greater transparency. Enhanced transparency enables both supply and demand side to understand a product's provenance and contributes to market forces for more secure products.

Finally, sustainable cybersecurity can enhance national security. The private sector owns and operates 80-90 percent of all ICTs; they also research and build them. As such, efforts to manage the use of ICTs must account for all stakeholders, which can limit the effectiveness of multilateral agreements around the misuse of ICTs. If the private sector builds and uses ICTs in a more sustainable manner, the ability for nation states to misuse them becomes more difficult, decreasing the likelihood and benefits of misuse. Thus, thinking sustainably about cybersecurity may ultimately constrain nation state misuse of ICTs. In addition, to the extent that lax security and privacy policies across the ecosystem have facilitated the current misuse of ICTs to undermine democracy, collective action to better secure these assets should be recognized as a reinforcement to democracy and a buttress against further attacks through ICTs. Sustainable cybersecurity supports and enables stable democracies.

Through sustainable cybersecurity practices, stakeholders around the world can be intentional as they participate in and contribute to the modern economy, whether in developing products and services, running a household, operating critical infrastructure, or formulating national policies. As a result, incorporating elements of sustainability management into cybersecurity will help reframe perceptions of cybersecurity from fear, uncertainty, and doubt to a more proactive mindset of opportunity, transformation, and dynamism. This shift, we assert, will in turn lead to improved cybersecurity practices by all stakeholders and ultimately a more secure, resilient, and enduring ICT ecosystem to support the modern economy. Through this collective effort, all stakeholders can have greater confidence and trust that information and communications technologies will securely support today's innovations beyond tomorrow.

The paper concludes with a set of priority actions each stakeholder group can take collectively to improve cybersecurity. In the coming months Public Knowledge will convene a series of discussions around the concept of sustainable cybersecurity, the legal and policy constraints to implementing such an approach, and the incentives that could spur rapid transition to sustainable cybersecurity.

Introduction

Increasingly, data, information, and the devices that process them are driving the global economy and enabling its growth. The digital economy, a subset of the overall economy, is set to experience exponential growth due to the development and adoption of interconnected things, also known as the "Internet of Things," or IoT. This new growth follows a decade (2006-2016) in which the digital economy grew at a rate faster than the overall economy, 5.6 percent compared to 1.5 percent per year.[2] The increase in data and its critical role in the global economy has led several, including White House Cybersecurity Coordinator Rob Joyce and *the Economist*, to analogize data to oil.[3] Joyce further noted that, in contrast to limited resources like oil, clean air, and water, when measured by the number of devices connecting to it, the internet is, at this time, unlimited.

Unfortunately, there is an evolving risk that threatens today's internet and the economic and social good that it supports. That threat is growing global mistrust of information and communications technologies (ICTs), which are a broad collection of interconnected devices, including but not limited to the colloquial internet. The 2018 RSA Privacy and Security report found that 78 percent of respondents limit the amount of personal information they put online or share with companies.[4] A 2015 Pew Research Center study presaged one reason for this practice: in addition to concerns about economic sectors that Americans associate with data collection and monitoring, "Americans also have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age."[5] And in 2016, the National Telecommunications Information Administration reported that lack of trust in internet privacy and security deters consumers from engaging in certain electronic transactions and other e-commerce activities.[6]

---

[2] *See* BUREAU OF ECONOMIC ANALYSIS, *Initial Estimates Show Digital Economy Accounted for 6.5 Percent of GDP in 2016*, BEA.GOV (March 15, 2018), https://blog.bea.gov/2018/03/15/initial-estimates-show-digital-economy-accounted-for-6-5-percent-of-gdp-in-2016/.

[3] *See* THE ECONOMIST, *The World's Most Valuable Resource Is No Longer Oil, But Data*, ECONOMIST.COM (May 6, 2017), https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource.

[4] *See* RSA, 2018 RSA PRIVACY & SECURITY REPORT 7 (2018), https://www.rsa.com/content/dam/en/e-book/rsa-data-privacy-report.pdf.

[5] Mary Madden & Lee Rainie, AMERICAN'S ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE 3 (Pew Research Center ed., 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/; *see also* CENTRE FOR INT'L GOVERNANCE INNOVATION, *2017 CIGI-Ipsos Global Survey on Internet Security and Trust*, CIGIONLINE (last visited Apr. 2, 2018), https://www.cigionline.org/internet-survey.

[6] *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security may Deter Economic and Other Online Activities*, NTIA (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

These studies, paired with near daily data breaches and other security headlines, remind us that the current approach to cybersecurity -- though increasingly more appropriately focused on risk management and less on compliance -- is still insufficient to secure the modern economy. It is, in a word: unsustainable. In addition to the risks presented by consumer-grade IoT,[7] the growing prevalence of smart cities and connected critical infrastructure further increases the dangers current cybersecurity practices pose to the longevity of the broader ecosystem. Add the trust challenges of "fake news" and the growth of artificial intelligence and the opportunities for strategic failure grow exponentially.

In short, we face a ticking time bomb as IoT emerges across economies thereby significantly expanding known cybersecurity challenges, and today's model for dealing with these developments underestimates their danger and under-invests in protection. We therefore believe a fundamental shift in approach, from short-term market signals to sustainability, is essential to minimize the likelihood of a calamity of public confidence that could undermine the modern economy and democratic institutions. Sustainable cybersecurity is an approach in which interactions with the ICT ecosystem are understood and deliberate, and where each participant understands its responsibility as a steward to respect and protect it to preserve its future use. Transitioning to a sustainability-style approach to cybersecurity will require the most powerful societal institutions to shift course without delay and in parallel, and includes commitments from (1) businesses to revise managerial approaches to better allocate investment strategies and assess profitability measurements (internalize externalities); (2) governments to evolve national strategies; (3) insurers to shift incentives through new underwriting parameters; (4) educational institutions to modernize curricula; and (5) consumers to learn the relevant elements of cybersecurity and build them into daily life.

This paper proposes that incorporating elements of sustainability management into cybersecurity will help reframe perceptions of cybersecurity from fear, uncertainty, and doubt to a more engaging mindset of opportunity, transformation, and dynamism. This shift, we assert, will in turn lead to improved cybersecurity practices by all stakeholders and ultimately a more secure, resilient, and enduring ecosystem to support the modern economy.[8] We reach this conclusion by outlining several key aspects of sustainability and considering their relevance and application in the context of cybersecurity. The paper concludes with a list of priority actions each stakeholder group can take collectively to improve cybersecurity.

---

[7] Malicious actors will increasingly use compromised IoT devices to launch global automated attacks. *See* The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Internet and Communications Resilience* 1 (Nov. 16, 2017), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

[8] *See* Maria Bada, Jason R.C. Nurse, and Angela Sasse, *Cyber Security Awareness Campaigns: Why do they fail to change behavior?*, GLOBAL CYBER SECURITY CAPACITY CENTRE (Sept. 15, 2016), https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/csss2015_bada_et_al.pdf.

Traditional approaches to cybersecurity are insufficient for the modern economy.

Security challenges have confronted users since the earliest days of interconnected networks. Network administrators initially used compliance-based approaches to address these challenges, which required administrators to complete a series of tasks, often checklists, to comply with established security requirements. However, scaling compliance to increasingly complex and expansive networks that include not only computers but also mobile and other smart devices has become increasingly less effective in securing interconnected networks. In recent years, in order to help prioritize the assets most critical to an organization's operations, the approach to cybersecurity has begun to shift from compliance to risk management. While risk management can be effective in reducing security risks to enterprise networks, it can be less useful in guiding organizations' decisions about the security of programs and devices that might form or connect to those networks, particularly for organizations whose offerings have suddenly become "connected." An effective approach to cybersecurity must expand the current understanding of the cybersecurity lifecycle to include inputs that can affect the operation of the network and the networks to which it connects.

Today's economy runs on data, and for too long a primary focus has been on connecting and collecting it without appropriate concern for protecting it. A number of factors have contributed to the present state. First, inadequate education and training – such as teaching information security in only narrow fields, if any – have contributed to poor hardware and software design and development procedures[9] and weak network architecture and protection. Next, business decisions to be first-to-market rather than secure-to-market have flooded the marketplace with products suffering from known vulnerabilities and little or no updatability. Finally, consumers have made choices with insufficient knowledge and understanding of product and service security and privacy features, forcing them to bear too much responsibility for the security of their data and the devices that generate it.[10]

The consequences of this short-term approach to cybersecurity appear regularly in newspapers around the world. The most critical of computer hardware was for decades vulnerable to acute security weaknesses;[11] multiple governments and organizations have had sensitive consumer personal data and proprietary corporate information

---

[9] *See* Brenden I. Koerner, *Inside the Cyberattack that Shocked the US Government*, WIRED (Oct. 23, 2016, 5:00 PM), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[10] *See generally* THE COUNCIL OF ECON. ADVISORS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY (Council of Economic Advisors, Feb. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. ("CEA Report").

[11] *See* Michael Lines, *Meltdown/Spectre: The First Large-Scale Example of a "Genetic" Threat*, DARKREADING (Feb. 20, 2018, 10:30 AM), https://www.darkreading.com/vulnerabilities---threats/meltdown-spectre-the-first-large-scale-example-of-a-genetic-threat/a/d-id/1331071?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple; *see also* Brad Chacos & Michael Simon, *Meltdown and Spectre FAQ: How the critical CPU flaws affect PCs and Macs*, PCWORLD (Feb. 22, 2018, 7:14 AM), https://www.pcworld.com/article/3245606/security/intel-x86-cpu-kernel-bug-faq-how-it-affects-pc-mac.html.

compromised;[12] and industrial control systems and other critical infrastructure have been unlawfully accessed by criminals and nation state actors.[13] More recently, poorly secured IoT has become a force multiplier for malicious actors who continue to expand the scale and impact of distributed denial-of-service (DDoS) attacks.[14]

Stakeholder misconceptions about market interest in security capabilities exacerbate the results of society's suboptimal choices. For example, a recent study of communications service providers (e.g., telecommunications carriers) and purchasers (e.g., enterprises such as corporations) found that enterprises were willing to pay a 15 percent premium to support compliance with secure internet routing practices (the process of transmitting packets over the internet).[15] The same study revealed that service providers underestimated the value their customers place on security and highlighted that providers' security posture is a characteristic to distinguish competitors.[16] This disconnect highlights the need for additional analysis of enterprise and consumer willingness to pay more for better security, and not just in the connectivity and transmission context. At the same time, it begs the question of whether or not they should have to. Security is a fact of doing business. Doing it right should not always have to cost enterprise customers and individual consumers more. But to date, doing it wrong has – perhaps most significantly in risking public trust in ICTs.

Together with these misperceptions, current market incentives do not support adequate cybersecurity investment and funding.[17] Often, the organizational victim of malicious cyber activity could have avoided or reduced its impact by investing in cybersecurity during procurement, employee training, and network design and management, to name but a few effective approaches. "When market incentives encourage manufacturers to feature security innovations as a balanced complement to functionality and performance, adoption of tools and processes that result in highly secure products is easier to justify."[18] The government, institutional investors, and other relevant

---

[12] *See* Michael Adams, *Why the OPM Attack Is Far Worse Than You Imagine*, LAWFARE (Mar. 11, 2016, 10:00 AM), https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine; *see also*, THE UNITED STATES DEP'T. OF JUSTICE, *US Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage,* JUSTICE.GOV (Nov. 27, 2017), https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

[13] *See* THE UNITED STATES DEP'T. OF JUSTICE, *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector,* JUSTICE.GOV (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged; *see also*, Joseph Berger, *A Dam, Small and Unsung, Is Caught Up In An Iranian hacking Case*, NEW YORK TIMES (Mar. 25, 2016), https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html.

[14] *See* Dan Gooden, *US service provider survives the biggest recorded DDoS in history*, ARSTECHNICA (Mar. 3, 2018, 4:24 PM), https://arstechnica.com/information-technology/2018/03/us-service-provider-survives-the-biggest-recorded-ddos-in-history/.

[15] *See* 451 RESEARCH, MANRS PROJECT STUDY REPORT 7 (Commissioned by Internet Society, Aug. 2017), https://www.routingmanifesto.org/wp-content/uploads/sites/14/2017/10/MANRS-451-Study-Report.pdf.

[16] *Id.* at 10.

[17] *See generally* CEA Report, *supra* note 10.

[18] THE SECRETARY OF COMMERCE AND THE SECRETARY OF HOMELAND SECURITY, A REPORT TO THE PRESIDENT ON ENHANCING THE RESILIENCE OF THE INTERNET AND COMMUNICATIONS ECOSYSTEMS AGAINST BOTNETS AND OTHER

stakeholders must emphasize that investment in cybersecurity in the early stage of a product or service development, as well as in network architecture and management, are more cost effective than attempting to bolt it on just before going to market, or failing to address it at all.[19]

Inadequate cybersecurity practices by governments and non-governmental organizations (NGOs) present a particularly pressing concern given the critical roles of such organizations in the ecosystem and in influencing public perceptions of trust.[20] Insecure networks risk not only becoming part of the problem, but also the target. Criminals and nation states can take advantage of vulnerabilities in networks to, for example, build a botnet,[21] which can be directed at any number of internet-connected devices, from home refrigerators to smart factories to medical devices, regardless of these targets' proximity. Given challenges in attributing cyber activity, poor cybersecurity practices by governments in particular can potentially exacerbate the consequences and further erode public trust in ICTs - if, for example, a government were to take action abroad in response to malicious activity enabled by a poorly configured system that has been compromised by actors operating in a third country. And yet, due to the increasingly prevalent role ICTs play in all aspects of society, the same concerns about unintended consequences could be said for almost all stakeholders' cybersecurity actions.[22]

Furthermore, the effects of the current unsustainable approach to ICT security threaten not only strong digital economies, but also nascent ones. Failure to trust and adopt ICTs, due in part to their insecurity, risks countries realizing the benefits these emerging digital populations could experience in the modern economy. At the same time, authoritarian regimes exploit insecure ICTs and their effects to develop legal systems that

---

AUTOMATED, DISTRIBUTED THREATS: DRAFT FOR PUBLIC COMMENT 23 (Jan. 5, 2018), https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf. ("Internet Resilience Draft Report").

[19] *See id.* at 33-34; *see also*, Robert Hawk, *DevSecOps: The Importance of Building Security from the Beginning*, DARKREADING (Mar. 9, 2018, 10:30 AM), https://www.darkreading.com/endpoint/devsecops-the-importance-of-building-security-from-the-beginning/a/d-id/1331210?_mc=sm_dr&hootPostID=4af20634b103363ab773998659c63368; Leigh-Anne Galloway, *A Secure Development Approach Pays Off*, DARKREADING (Mar. 2, 2018, 10:30 AM), https://www.darkreading.com/application-security/a-secure-development-approach-pays-off/a/d-id/1331154?ngAction=register&ngAsset=389473.

[20] *See, e.g.*, Dante Disparte, *Cities Held For Ransom - Lessons From Atlanta's Cyber Extortion*, FORBES (Apr. 2, 2018, 9:30 AM), https://www.forbes.com/sites/dantedisparte/2018/04/02/cities-held-for-ransom-lessons-from-atlantas-cyber-extortion/#54f4d935996b; Ajay Bhalla, Bhaskar Chakravorti, & Ravi Shankar Chaturvedi, *The 4 Dimensions of Digital Trust, Charted Across 42 Countries*, HARVARD BUSINESS REVIEW, https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries (Feb. 19, 2018).

[21] *See, e.g.*, UNITED STATES DEP'T. OF HOMELAND SECURITY, THE INCREASED THREAT TO NETWORK INFRASTRUCTURE DEVICES AND RECOMMENDED MITIGATIONS (National Cybersecurity and Communications Integration Center, Aug. 30, 2016), https://cyber.dhs.gov/assets/report/ar-16-20173.pdf; UNITED STATES DEP'T. OF HOMELAND SECURITY, Binding Operational Directive BOD-16-02, Threat to Network Infrastructure Devices (DHS Sept. 27, 2016), https://cyber.dhs.gov/assets/report/bod-16-02.pdf.

[22] *See* Danny Palmer, *Ransomware for robots is the next big security nightmare*, ZDNET (Mar. 9, 2018, 7:47 AM), http://www.zdnet.com/article/ransomware-for-robots-is-the-next-big-security-nightmare/.

undermine privacy in the name of security. These governmental policies can take many forms, from unchecked access to communications' metadata and content to data localization and source code requirements, any one of which can undermine security and privacy and thereby public trust in information and communications technologies. Stakeholders' failure to address ICT security challenges throughout the ecosystem may cost emerging digital economies the opportunity to see the true economic and social benefits interconnection can bring.

Even well intentioned regulatory efforts that directly and indirectly improve cybersecurity, e.g., the General Data Protection Regulation (GDPR), can fall short.[23] Although the results of these efforts are not yet calculable, this varied regulatory landscape presents challenges for organizations operating internationally and highlights the limitations national and regional regulatory regimes face in truly enhancing cybersecurity on a global scale.

These shortfalls and limitations evidence a need for a more holistic approach to ICT security and privacy. Public and private organizations and consumers should collaborate to identify best practices and frameworks that transcend boundaries, national laws, and cultures to create a cohesive ICT security agenda to sustain the modern economy into the future. An enduring approach should view the security of ICTs and associated privacy enhancements as critical to their sustainability, and thus the sustainability of the modern economy. As Palo Alto Networks CEO, Mark McLaughlin, has cautioned, "The life of the digital age is literally at risk if we don't advance security prevention."[24]

Recent developments portend a more holistic approach to cybersecurity.

In recent months, in part as a result of growing distrust in ICTs,[25] many cybersecurity firms, among other organizations, are beginning to extol the broader importance of cybersecurity, and it is not just to sell more goods and services. Rather, they recognize that cybersecurity is essential to the modern economy, and that weak security is eroding public trust in the tools that enable it. In late 2017, a cybersecurity company CEO remarked that "what cybersecurity companies know should be a public good."[26] This belief reflects that of a growing number of public and private organizations who describe cybersecurity as a shared responsibility. In terms quite similar to environmental

---

[23] Lincoln Kaffenberger, Emanuel Kopp, & Christopher Wilson, *Cyber Risk, Market Failures, and Financial Stability*, Int'l Monetary Fund Working Paper 185 (2017), at 17, 30 ("The regulatory regime should encourage ongoing vigilance by boards and senior management to build resilience through investment in cyber security while giving institutions flexibility to address the risks in the way they see as optimal. However, actions by individual countries—and by financial sector participants alone—will not be sufficient.").

[24] *See* David Needle, *Palo Alto Networks CEO "Next Gen Security Solutions Must Restore Trust"*, RSACONFERENCE (Mar. 3, 2016), https://www.rsaconference.com/blogs/palo-alto-networks-ceo-nex-gen-security-solutions-must-restore-trust.

[25] *See, e.g.*, Stephanie Johnson, *Palo Alto Networks Academy: Protecting Life in the Digital Age One Student at a Time*, PALOALTO NETWORKS (Feb. 26, 2018, 1:00 PM), https://researchcenter.paloaltonetworks.com/2018/02/palo-alto-networks-academy-protecting-life-digital-age-one-student-time/ ("Cybersecurity is essential to maintaining trust in our digital way of life.").

[26] Needle, *supra* note 24.

stewardship – a field known for its sustainability practices, a recent report for the Internet Society noted the "value of contributing to the overall security of the internet community"[27] in highlighting the benefits of implementing internet routing best practices.

Public recognition of the need for collaborative actions to improve cybersecurity extends well beyond cybersecurity firms. At the 2018 World Economic Forum (WEF), WEF announced the Global Centre for Cybersecurity. Its foci include establishing an independent library of cyber best practices; helping partners to enhance knowledge on cybersecurity; working towards an appropriate and agile regulatory framework on cybersecurity; and serving as a laboratory and early-warning think tank for future cybersecurity scenarios.

A few weeks later, at the 2018 Munich Security Conference, several multinational corporations announced 10 principles in the Charter of Trust for a Secure Digital World. These principles range from education and security by design to transparency and response.[28] The press release emphasizes the roles of governments and companies in taking decisive action: "[t]his means making every effort to protect the data and assets of individuals and businesses; prevent damage from people, businesses and infrastructures; and build a reliable basis for trust in a connected and digital world."[29]

In the United States, in March 2018, several businesses formed the Coalition to Reduce Cyber Risk, which "aims to enhance cybersecurity and support economic growth by partnering across industry and with governments around the world to strengthen and align approaches to improving cybersecurity risk management." That same month two trade associations formed the Council to Secure the Digital Economy, which will "pursue security mitigation as intensely as digital innovation. [The Council] will determine a distinct set of priorities and industry initiatives, working in partnership with the public sector both in the U.S. and globally."[30]

At the 2018 annual RSA cybersecurity conference, 34 technology and security companies announced the Cybersecurity Tech Accord. Companies signing the Tech Accord commit to equal protection for customers worldwide. These protections include mounting a stronger defense of customers, regardless of the motivation for attacks online; refraining from assisting governments launch cyberattacks and protecting against tampering and exploitation of products and services through development, design, and distribution; building capacity to empower developers and technology users to better protect themselves; and acting collectively through formal and informal partnerships with industry, civil society, and security researches to enhance security information sharing and vulnerability disclosure.[31]

---

[27] 451 Research, *supra* note 15 at 10.
[28] *See* SIEMENS, *Charter of Trust* (2018), https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf.
[29] *Id.*
[30] *USTelecom and ITI Launch Council to Secure the Digital Economy*, USTELECOM.ORG (Feb. 23, 2018), https://www.ustelecom.org/news/press-release/ustelecom-and-iti-launch-council-secure-digital-economy.
[31] https://cybertechaccord.org.

The insurance market is also beginning to broaden its approach to assessing cyber risk. In early 2018, Allianz Global Corporate & Specialty (AGCS) announced a partnership with global risk consulting firm Aon PLC and technology companies Apple and Cisco. AGCS will offer discounted cyber insurance policies to companies that submit to a risk assessment and use identified technology products. The effort demonstrates the broader shift in cybersecurity from compliance to risk management, which extends risk evaluation beyond the insured's network operations to its engagements with the ecosystem to address security "more holistically."[32]

Governments, too, are increasingly calling for greater cybersecurity action for the collective good. These calls echo sustainability management practices such as reducing pollution and framing responsible business development choices as investments. For example, in implementing Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, the U.S. National Telecommunications and Information Administration seeks to develop a pathway toward "an adaptable, sustainable, and secure technology market." It also called on companies not only to avoid carrying malicious internet traffic, but also to make public such decisions. Similarly, the 2015 Japanese Cybersecurity Strategy concisely observes:

> [i]n bringing products and services in which high level security is assured as a quality feature to the market, and in making management decisions for new business creation, cybersecurity knowledge has become a basic competency required for enterprise senior executives. For the enhancement of Japan's socio-economic vitality as well as sustainable development, it is necessary that more enterprise senior executives will grasp such societal changes precisely, and raise awareness of cybersecurity measures not as inevitable "cost" of business but as an "investment" for more progressive management.[33]

More recently, the White House Council of Economic Advisors stated plainly that "[c]ybersecurity is a common good…[that] weak cybersecurity carries a cost not only to the firm itself but also to the broader economy through the negative externalities imposed on the firm's customers and employees and on its corporate partners."[34] Suffice to say, nascent but exponential growth in IoT will likely compound these externalities absent a significant shift in stakeholder behavior.

To address these challenges, several organizations, both public and private, are calling for a cybersecurity moonshot along the lines of the government-led effort

---

[32] Allison Grande, *Apple Cisco Partner with Insurers for Novel Cyber Coverage*, Law360 (Feb. 6, 2018, 10:40 PM), https://www.law360.com/articles/1009760/apple-cisco-partner-with-insurers-for-novel-cyber-coverage.

[33] THE GOV'T. OF JAPAN, CYBERSECURITY STRATEGY 12, 14-15 (Sept. 4, 2015), https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

[34] CEA Report, *supra* note 10 at 21.

that culminated in the first lunar landing.[35] While potentially a helpful motivating frame, there are also limitations to the moonshot concept in the context of cybersecurity, in part because it is a continuous combination of actions. For example, given the impact of Moore's law and other innovation attributes of these technologies, will a cybersecurity moonshot ever be complete? How does a cybersecurity moonshot account for the role of consumers? And how does it address supporting elements, such as the need to expand and enhance cybersecurity education?

Sustainable cybersecurity to secure the modern economy.

In addition to a cybersecurity moonshot, stakeholders – governments, corporations, educators, and consumers – need to reframe their approach to cybersecurity to one of sustainability. Sustainability acknowledges roles for a range of stakeholders and recognizes the need to manage and engage today in order to ensure the same or better opportunities tomorrow. Sustainability encompasses supply chain management, interoperability and scalability, consumer engagement, and in some areas regulatory compliance. In the context of cybersecurity, it could transform corporate and consumer perceptions from costs of time and money to savings and features, and meaningfully translate these attributes to the market.

Gaining recognition in the mid-90s, the modern sustainability movement developed to enable organizations to optimally operationalize their interactions with public goods.[36] Today, the field of sustainability management seeks to integrate an understanding of "the physical dimensions of sustainability" into routine management decision-making. The field teaches tomorrow's CEOs to manage their organization's waste, use of energy, water, and other raw materials to ensure sustainability throughout supply chains, and to be aware of the financial risks posed by environmental accidents, pollution, and climate change.[37] Sustainability management "continues to study conservation and pollution, but now encompasses a far broader set of concerns and has come to include the built environment, management, and the transition to sustainable cities."[38]

---

[35] *See, e.g.*, Shaun Waterman, *What is a "cyber moonshot" anyway?*, CYBERSCOOP (Oct. 19, 2017), https://www.cyberscoop.com/cyber-moonshot-accenture-gus-hunt/; Sean Morgan, *Call for a Cybersecurity "Moonshoot" Dominates First-Ever Government Ignite*, PALOALTO NETWORKS (Oct. 27, 2017), https://researchcenter.paloaltonetworks.com/2017/10/gov-call-cybersecurity-moonshot-dominates-first-ever-federal-ignite/.

[36] *See, e.g.*, Rebecca Tuhus-Dubrow, *"Sustainability" is older than you think*, BOSTONGLOBE.COM (Dec. 7, 2014), https://www.bostonglobe.com/ideas/2014/12/07/sustainability-older-than-you-think/qCjnEzwtxmBjxebceg8OzL/story.html ("Sustainability is about having a vision for the future. And environmentalism is about dealing with problems that have led us up to the present day. It's about the past and the present. And I think sustainability says, OK. We screwed it all up. We know that emissions are a big problem, we know that water pollution is a problem....Now what?").

[37] Steven Cohen, *The Evolution of Sustainability Education*, HUFFPOST (May 22, 2017, 8:25 AM), https://www.huffingtonpost.com/entry/the-evolution-of-sustainability-education_us_5922d872e4b0e8f558bb282e.

[38] *Id.*

For BlackRock, a large institutional investor, "sustainability means long-term thinking in every respect, whether it be reducing our energy consumption, contributing to communities or building better financial futures for our clients. It is about responsible decision-making."[39] BlackRock's CEO, Larry Fink, observed that society expects responsible decision-making: "[t]o prosper over time, every company must not only deliver financial performance, but also show how it makes a positive contribution to society. Companies must benefit all of their stakeholders, including shareholders, employees, customers, and the communities in which they operate."[40] BlackRock sees increasing societal expectations that corporations "serve a social purpose."[41]

This responsible decision-making approach benefits shareholders in addition to society. Indeed, analysis of Fortune 500 companies makes clear that sustainable companies are successful, often very successful, companies. Thus, contrary to common perceptions that sustainability takes away from companies' profits, in fact, sustainable companies are more successful than their peers that have not adopted sustainable practices.[42] The reasons for this success are beyond the scope of this paper. However, in most CEOs' and organizational leaders' evaluation of priorities, whether recognized by these leaders or not, there is one element that enables or risks all of the others: cybersecurity. Yet, recent research indicates that financial benefits can also result for companies that adopt responsible cybersecurity practices.[43] Sustainable cybersecurity is essential to achieving shareholder value and a social purpose.

Beyond profitability, organizations should begin to frame their cybersecurity activities in a sustainable way for several reasons. To begin, ICTs underpin almost every

---

[39] BLACKROCK, *BlackRock Responsibility: Environmental Sustainability*, BLACKROCK (last visited Mar. 12, 2018), https://www.blackrock.com/corporate/en-us/responsibility/environmental-sustainability.
[40] BLACKROCK, *Larry Fink's Letter to CEO's: A Sense of Purpose*, BLACKROCK (last visited Feb. 21, 2018), https://www.blackrock.com/corporate/en-us/investor-relations/larry-fink-ceo-letter.
[41] *Id.*
[42] *See*, *e.g.,* Carly Fink & Tenise Whelan, *The Comprehensive Business Case for Sustainability*, HARVARD BUSINESS REVIEW (October 21, 2016), https://hbr.org/2016/10/the-comprehensive-business-case-for-sustainability; Eccles, Iannou & Serafeim, THE IMPACT OF CORPORATE SUSTAINABILITY ON ORGANIZATIONAL PROCESSES AND PERFORMANCE 19 (Harvard Business School, Nov. 2014), http://www.hbs.edu/faculty/Publication%20Files/SSRN-id1964011_6791edac-7daa-4603-a220-4a0c6c7a3f7a.pdf. ("Overall, we find evidence that firms in the High Sustainability group are able to significantly outperform their counterparts in the Low Sustainability group. This finding suggests that companies can adopt environmentally and socially responsible policies without sacrificing shareholder wealth creation. In fact, the opposite appears to be true: High Sustainability firms generate significantly higher stock returns, suggesting that indeed the integration of such issues into a company's business model and strategy may be a source of competitive advantage for a company in the long-run. A more engaged workforce, a more secure license to operate, a more loyal and satisfied customer base, better relationships with stakeholders, greater transparency, a more collaborative community, and a better ability to innovate may all be contributing factors to this potentially persistent superior performance in the long-term.").
[43] *See* Ayman Sayed, *Why Security-Driven Companies Are More Successful*, DARKREADING (Mar. 7, 2018, 10:30 AM), https://www.darkreading.com/operations/why-security-driven-companies-are-more-successful/a/d-id/1331173; Steven Chabinsky, *The Top 12 Practices of Secure Coding,* SECURITY MAGAZINE (Jan. 1, 2018), https://www.securitymagazine.com/articles/88600-the-top-12-practices-of-secure-coding; Scott J. Shackelford, Timothy L. Fort, & Danuvasin Charoen, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995, 2020 (2016).

modern day transaction, from the delivery of electricity and water to banking, shopping, manufacturing, and correspondence. As such, organizations develop, transmit, and have access to vast amounts of information, including very sensitive data in the form of proprietary and personally identifiable information. As is increasingly apparent, failure to ensure the confidentiality, integrity, authenticity, or availability of aspects of this information – actions most commonly described as cybersecurity or information security – can result in critical failures for associated and unrelated information, devices, and actions. These failures risk reputation, income, assets, and the very longevity of the organization as a going concern.[44] Left unchecked, poor cybersecurity can also threaten ICTs themselves. "Even though [ICTs] are not a natural resource – like air, land, sea, or space – they can be ruined beyond use by careless actions. In fact, as their foundation is not natural, but essentially built on human trust, cyberspace and the internet may be far more sensitive to long-term pollution and disruption."[45]

As a result, like sustainability, cybersecurity is slowly but increasingly becoming a "C-suite" issue. Just as past business operations may have contributed to climate change and other traditional sustainability challenges, many of today's cybersecurity issues are the result of business practices that failed to adequately consider the broader implications of a particular decision. Rushing products with known vulnerabilities to market in order to be first rather than secure-to-market has resulted in an ecosystem populated with thousands of vulnerable consumer devices and industrial control systems.[46] And like other sustainability issues, the externalities of vulnerable devices and applications, whether embedded in home security cameras or critical infrastructure, can have significant, if latent, consequences, particularly when malicious actors exploit more than one vulnerability at once or as part of a broader campaign.[47]

The sustainability movement and cybersecurity also have in common the opportunities and challenges of interoperability and scale. Sustainability policy emerged from the need for global collective action. In recent decades, large groups of stakeholders across the world have adopted sustainability policies and programs to tremendous effect.[48]

---

[44] *See* Dune Lawrence, *A Leak Wounded This Company. Fighting the Feds Finished It Off*, BLOOMBERG (Apr. 25, 2016), https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/; PRO ONCALL TECHNOLOGIES, *3 Companies that Went out of Business Due to a Security Breach*, Pro On-Call Business (Nov. 6, 2014), https://prooncall.com/3-companies-went-business-due-security-breach/.

[45] Jason Healey, A NONSTATE STRATEGY FOR SAVING CYBERSPACE 29 (Frederick Kempe et al. eds., Atlantic Council Strategy Papers No. 8, 2017).

[46] Robert Lemos, *IoT Security, Easy to Compromise, Not So Easy to Fix*, SYMANTEC (Oct. 23, 2017), https://www.symantec.com/blogs/corporate-responsibility/iot-security-easy-compromise-not-so-easy-fix; Lucian Constantin, *Critical Bluetooth Flaw Puts Over 5 Billion Devices at Risk for Hacking*, FORBES (Sept. 12, 2017, 9:23 AM) https://www.forbes.com/sites/lconstantin/2017/09/12/critical-bluetooth-flaws-put-over-5-billion-devices-at-risk-of-hacking/#72abf0c868b1.

[47] *See* Lily Hay Newman, *The Botnet that Broke the Internet Isn't Going Away,* WIRED (Dec. 9, 2016, 7:00 AM), https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/.

[48] *See* UNITED NATIONS GLOBAL IMPACT, 2017 UNITED NATIONS GLOBAL COMPACT PROGRESS REPORT 25 (UN Global Impact, 2017), https://www.unglobalcompact.org/docs/publications/UN%20Impact%20Brochure_Concept-FINAL.pdf.

Similarly, ICT interoperability, ensuring that products work regardless of the country or network to which they connect, has fostered an ever-expanding global marketplace and strong economic growth. Yet, as discussed throughout this paper, that marketplace and associated growth are at risk from growing distrust of ICTs due in part to their inadequate security. In order to strengthen that trust, organizations across the ecosystem must do their part. Sustaining cybersecurity in the modern economy means being intentional about interoperability and the business choices that should be made to securely enable it.[49]

Noteworthy, too, is the critical role cybersecurity plays in core sustainability practices. As with most operations today, information and communications technologies increasingly, if not completely, support traditional sustainability actions as identified by the United Nations Global Compact 10 Principles and the 17 Sustainable Development Goals.[50] Cybersecurity is essential to achieving each of these Principles and Goals. For example, climate action cannot be assessed without gathering data and analyzing it. Identifying the security vulnerabilities in such scientific collection and assessment is no small undertaking. Yet ensuring the integrity, authenticity, and availability of such data from numerous collection points is critical to developing effective options to address the challenge. Relatedly, supply chain management, a crosscutting issue critical to ensuring business operations, also depends upon the integrity, authenticity, and availability of relevant information. Short of becoming a universal Goal in itself, implementing sustainable cybersecurity practices could be a supplement to Goal Nine: "Build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation."

Furthermore, the cybersecurity nexus to these now commonplace business practices suggests organizations' existing sustainability processes and policies likely provide a foundation upon which to incorporate and scale enhanced approaches to cybersecurity.[51] In addition to operational tracking and compliance to achieve desired objectives – environmental impact or, in the future, secure and stable code – these sustainability policies also enable organizations to be more transparent about their decisions. This transparency has helped investors and consumers to make more informed decisions and better evaluate competitors. Metrics about theses policies and their results are so valuable to investors that some stock exchanges now require them in the form of environmental, social, and governance (ESG) integrated reports.[52]

---

[49] *See* Johnson *supra*, note 25.

[50] *See* UNITED NATIONS GLOBAL COMPACT, *The 10 Principles of the UN Global Compact*, UNGLOBALCOMPACT.ORG, https://www.unglobalcompact.org/what-is-gc/mission/principles (last visited, Apr. 2, 2018); *See also*, UNITED NATIONS GLOBAL COMPACT, *How Your Company Can Advance Each of the SDGs*, UNGLOBALIMPACT.ORG, https://www.unglobalcompact.org/sdgs/17-global-goals. (Last visited Apr. 2, 2018). Consider also that assessing the number of displaced persons due to conflict also requires accurate and available data; in some situations that data must also be kept confidential from controlling regimes that may be targeting certain populations.

[51] *See* Joseph Marks, *DHS To Scrutinize Government Supply Chain For Cyber Risks*, NEXTGOV (Feb. 14, 2018), http://www.nextgov.com/cybersecurity/2018/02/dhs-scrutinize-government-supply-chain-cyber-risks/145998/; Kristin Goodwin & Paul Nicholas, DEVELOPING A NATIONAL STRATEGY FOR CYBERSECURITY 13 (Microsoft, Oct. 2013), https://www.microsoft.com/en-us/cybersecurity/default.aspx.

[52] *See* Christopher P. Skroupa, *ESG Reporting Reshapes Global Markets*, FORBES (Apr. 24, 2017), https://www.forbes.com/sites/christopherskroupa/2017/04/24/esg-reporting-reshapes-global-

A similar approach to transparency about cybersecurity policies and practices could have meaningful impact. "Greater awareness and use of transparency tools and practices [will] allow both the supply side and demand side to understand what goes into IoT products, generate market forces for better security through transparency, and increase assurances that no known vulnerabilities are shipped with products."[53] Where currently securities exchanges require organizations to provide information on material cybersecurity issues, in the future, due to increasing regulations around cybersecurity, companies' cybersecurity public reporting obligations will expand. As integrated reporting matures, rather than inclusion of cybersecurity activities simply fulfilling a reporting requirement, in light of its strategic importance to traditional ESG elements outlined above, cybersecurity should become an integrated reporting cornerstone.[54]

In the interim, organizations should build upon recent efforts toward greater transparency about cybersecurity. In addition to the coalitions and centers described above, some companies, including Intel, already discuss their security and privacy practices in the broader context of their public policy work. Intel notes that "trust in the global digital economy is contingent upon providing robust security and a high level of privacy protection."[55] And the U.S. government has begun to share details about security vulnerabilities in its network.[56] Furthermore, over the years, computer hardware manufacturers have taken steps to make physical production more sustainable by extending the lifespan and recyclability of their products,[57] which further suggests – in addition to the recently announced efforts – that the technology sector may be a good starting point and partner in extending sustainability practices to incorporate cybersecurity.

---

markets/#71bdf9ff5d5e; *see also* Timothy F. Slaper & Tanya J. Hall, *The Triple Bottom Line: What Is It and How Does It Work?*, INDIANA BUSINESS REVIEW (Spring 2011), http://www.ibrc.indiana.edu/ibr/2011/spring/article2.html; *see generally* Global Reporting Institute, https://www.globalreporting.org/information/about-gri/Pages/default.aspx.

[53] *See* Internet Resilience Draft Report, *supra* note 18 at 26, 28.

[54] The integrated report shows how a reduction in greenhouse gas impacts profitability, logistics, the supply chain, the value chain, etc. *See* Skroupa, *supra* note 52.

[55] Intel Public Policy: Security and Privacy, https://www.intel.com/content/www/us/en/policy/policy-security-privacy.html (last visited Feb. 23, 2018); *see also* Intel 2016 Corporate Responsibility Report, https://www.intel.com/content/www/us/en/corporate-responsibility/corporate-responsibility.html (last visited Feb. 23, 2018).

[56] *See* Letter from Senator Ron Wyden to Christopher C. Krebs, Department of Homeland Security (Sept. 21, 2017), https://www.wyden.senate.gov/imo/media/doc/letter%20to%20DHS%20Regarding%20NPPD's%20Kasperksy%20BDO.pdf.

[57] *See* Nathaniel Bullard & Adam Minter, *The Upside to America's Gadget Infatuation*, BLOOMBERG (Dec. 29, 2017, 12:00 PM), https://www.bloomberg.com/view/articles/2017-12-29/the-upside-to-america-s-gadget-infatuation ("Companies such as HP Inc. and Dell Inc. are leading the way with designs that extend the lifespan of devices and enable recyclers to extract materials affordably. That's good news for consumers, and even better news for the environment."); *see also* 2017 Impact Report at 19, SUSTAINABILITY CONSORTIUM (last visited Apr. 17, 2018), https://www.sustainabilityconsortium.org/impact/impact-report/ ("The computer category in particular has benefited from broadly adopted eco-certifications, like ENERGY STAR(c) and EPEAT, which has helped drive sector manufacturers to focus on the key sustainability issues within their own operations and their suppliers.").

Nascent efforts are already underway to increase transparency, raise consumer privacy and security awareness, and foster demand for better products and services. A group of technology security and corporate accountability experts together with Consumer Reports are developing "The Digital Standard" to create a digital privacy and security standard to help guide the future design of consumer software, digital platforms and services, and internet-connected products.[58] Established software development best practices and efforts to develop a software bill of materials also support an informed marketplace. Just as consumers now look to ingredient labels and business practices around environmental impact and child labor before buying products, greater transparency and awareness about entities' cybersecurity practices through efforts such as the Digital Standard will better educate consumers, who will begin to demand products that put security first.[59] Attendant to this demand, and also elements of the Standard, are improved information policies and practices that clearly convey to the network operator, device owner, and end user, in plain language that the average person can comprehend, what data the device is collecting and to what purposes the data will be put.[60]

As the internet adds hundreds if not thousands of new devices every day, it is past time for the organizations developing them and the purchasers that buy them to agree they must be developed and maintained in as secure a manner as possible. In the future, organizations that compete on security can reap many of the same benefits as organizations that adopted sustainability practices, perhaps most importantly growing the economy by doing well and doing good. The economy of the future depends on products and services that compete both on security and functionality.

So, too, does our national security. The 2018 Director of National Intelligence threat assessment highlights quite succinctly the urgency to act: "[t]he potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—*with relatively little built-in security*—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits."[61]

For years senior military and intelligence leaders have recognized the importance of sustainability to national security.[62] Far from a limitation in the context of national security, here, too, a sustainable approach to cybersecurity has merit. In evaluating the national security implications of framing cybersecurity as a sustainability issue, several facts must

---

[58] *See generally* The Digital Standard, https://www.thedigitalstandard.org.
[59] *See* Internet Resilience Draft Report, *supra* note 18 at 19.
[60] *Id.* at 24 ("Customer-supported profiles appropriate for home and industrial applications would provide a signal to the market that the customers will prefer IoT devices that meet the baseline. The profiles would also provide immediate opportunity for product differentiation.").
[61] Daniel R. Coats, WORLDWIDE THREAT ASSESSMENT 5 (Office of the Director of National Intelligence, Feb. 13, 2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf. (emphasis added).
[62] *See, e.g.*, Benjamin Schneider, *Defense Secretary Hagel reaffirms climate change, sustainability are central military concerns*, ENVIRONMENTAL DEFENSE FUND (Nov. 24, 2013), https://www.edf.org/blog/2013/11/24/defense-secretary-hagel-reaffirms-climate-change-sustainability-are-central.

be kept in mind. To begin, the private sector owns and operates between 80-90 percent of all ICTs; they also research and build them. Next, efforts to manage the use of ICTs must account for all stakeholders, which is where multilateral agreements around the misuse of ICTs face significant limitations. If the private sector builds and uses ICTs in a more sustainable manner, the ability for nation states to misuse them becomes more difficult, decreasing the likelihood and benefits of misuse.[63] Thus, thinking sustainably about cybersecurity may ultimately constrain nation state misuse of ICTs.

In addition, disagreements over the management of resources contribute to many national security threats.[64] In this case, the resource could be considered the (mostly) open internet and the ICTs with which it interoperates. For some governments the internet is a tool to advance democracy and economic development while, from an authoritarian viewpoint, it is a threat to regime stability that must operate under strict controls set by the state. If one assesses that lax security and privacy policies across the internet ecosystem facilitated in part the current misuse of ICTs to undermine democracy, voluntary and where necessary tailored regulatory actions that incorporate sustainability principles can better secure these assets. Such efforts should be recognized as reinforcements to democracy and a buttress against further attacks through ICTs. Sustainable cybersecurity supports and enables stable democracies.

Conclusion

Despite its known insecurities, the rise of the Internet of Things and our increasing dependence on it, together with growing distrust in information and communications technologies, necessitate a fundamental reformulation of the societal approach to cybersecurity in order for the digital age to continue its exponential growth. "'Cybersecurity' on its own has no time horizon, no easy way to make tradeoffs between today's needs and those of the future. Sustainability, wanting future generations to have an Internet that is as rich, open, and secure as the one today, is the easiest way to address these issues."[65] Treating cybersecurity as a sustainability issue will build upon the adaptive

[63] Consider recent action by the Chinese government to mitigate climate change. In the past the government pursued economic growth at the cost of the environment; faced with rising death tolls and other domestic impacts, the government radically changed course and began an aggressive effort to limit pollution. *See*, *e.g.*, Kearns, Dormido & McDonald, *China's War on Pollution Will Change the World*, BLOOMBERG (Mar. 9, 2018), https://www.bloomberg.com/graphics/2018-china-pollution/?cmpId=flipboard; Yanzhong Huang, *Why China's Good Environmental Policies Have Gone Wrong*, THE NEW YORK TIMES (Jan. 14, 2018), https://www.nytimes.com/2018/01/14/opinion/china-environmental-policies-wrong.html.

[64] *See e.g.*, Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community* 13 (Office of the Director of National Intelligence, May 11, 2017), https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf; James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community* 13-14 (Office of the Director of National Intelligence, Feb. 25, 2016), https://www.dni.gov/files/documents/Newsroom/Testimonies/HPSCI_Unclassified_2016_ATA_SFR-25Feb16.pdf ("Extreme weather, climate change, environmental degradation, related rising demand for food and water, poor policy responses, and inadequate critical infrastructure will probably exacerbate—and potentially spark—political instability, adverse health conditions, and humanitarian crises in 2016.").

[65] Healey, supra note 45 at 36-7.

and scalable nature of the sustainability movement. Independently, these operational approaches have evolved alongside rapid technological innovation, demonstrating their importance and endurance; bringing them together will further strengthen their effectiveness.

From this expansive viewpoint, one can begin to envision what sustainable cybersecurity means – it is more than just actions taken by developers and manufacturers of hardware and physical goods companies. Incorporating sustainable cybersecurity management practices throughout the internet and ICT ecosystem enables all stakeholders to do their part to enhance the ecosystem's security and reinforce trust in it. Through sustainable cybersecurity practices, stakeholders globally can be intentional as they participate in and contribute to the modern economy, whether in developing products and services, running a household, operating critical infrastructure, or developing national policies. Through this collective effort, all stakeholders can have greater confidence that information and communications technologies will securely support today's innovations beyond tomorrow.

Operationalizing Sustainable Cybersecurity

What follows are prioritized but not exhaustive actions stakeholders across the internet ecosystem can take and work toward to build and sustain a more resilient network of networks, one that protects the security and privacy of the data driving the modern economy.

For product manufacturers:

- Following secure software development best practices, e.g., Software Assurance Marketplace; OWASP
- Publishing a software bill of materials that details the product development process
- Establishing a product's usage, lifespan, and end-of-life management
  - Using the Manufacturer Usage Description Specification
  - Updating purchasers when a product exceeds its supported life
  - Offering discounted upgrades to reduce population of insecure products
  - Ensuring where appropriate products fail safe to safe/secure mode
- Selling products that are secure by design with no known defects
- Developing vulnerability management and patch dissemination policies and processes, including automatic updates where appropriate
- Participating in information sharing and analysis organizations
- Educating workforce about cybersecurity, including application outside the work environment

For enterprise network operators:

- Utilizing the NIST Cybersecurity Framework – identify, protect, detect, respond, recover
  - Including the supporting policies and procedures, e.g., incident response plan
- Requiring a software bill of materials for purchases of internet-connected devices
- Validating the integrity of hardware and software
- Developing patch management processes to ensure products remain up to date
- Maintaining least privilege across the network
- Securing access to infrastructure devices
- Segregating networks and functions
- Using Domain Message Authentication Reporting and Conformance (DMARC)
- Implementing Best Common Practice 38 & 84 - ingress and egress filtering
- Participating in information sharing and analysis organizations
- Educating workforce about cybersecurity, including application outside the work environment

For civil society and consumers:

- Educating themselves about cybersecurity
- Practicing good cyber hygiene
    - Backing up data
    - Installing updates when informed by manufacturers
    - Using strong passwords and not reusing them
    - Using two-factor authentication
    - Reducing opportunities to be a victim of social engineering
    - Using web browsers that filter bad domains
- Reinforcing good hygiene with friends and family
- Investing in products with robust security, as evidenced by, for example, the Digital Standard
- Holding accountable organizations that fail to adequately develop and secure products by using their competitors, where available

For governments:

- Leading by example in procurement, enterprise operations, personnel and national education, and research and development
- Convening stakeholders to build cybersecurity capacity internationally
- Supporting and participating in international standards organizations
- Improving incentives for stakeholders to implement sustainable cybersecurity, including by reevaluating liability frameworks
- Collaborating to investigate and whenever possible prosecute criminal misuse of ICTs
- Refraining from activities that undermine public trust in ICTs

Next steps

We propose to facilitate and participate in a series of multistakeholder conversations about this paper and the actions it outlines. Agenda items for these conversations include:

- Are these the right actions for these actors? What's missing?
- What are the legal and/or policy challenges limiting these actions' implementation?
- What incentives could spur broader adoption of these actions?
- Which actions would make useful case studies?