Microsoft

CYBERSPACE 2025

TODAY'S DECISIONS, TOMORROW'S TERRAIN

NAVIGATING THE FUTURE OF CYBERSECURITY POLICY

AUTHORS
David Burt
Aaron Kleiner
J. Paul Nicholas
Kevin Sullivan

JUNE 2014

Contents

"Real generosity toward the future lies in giving all to the present." – Albert Camus

Foreword

The world will experience extraordinary changes in the next decade, with growth the common element in these changes. In cyberspace, growth means more people, more devices, more connectivity, and more data. But there is significantly more to the story than just bigger numbers. The growth in cyberspace is not just a natural expansion of current patterns. It is driven and shaped by a number of external factors, many of which can be amplified or influenced by public policy choices.

This report, *Cyberspace 2025: Today's Decisions, Tomorrow's Terrain*, attempts to look over the horizon and see beyond technological trends to anticipate future catalysts for change. Cloud computing, the Internet of Things, big data, and cybersecurity loom large on today's—and tomorrow's—agenda. But what are the transformative elements that will define the future terrain of cyberspace? How will public policies impact potential growth? What are the tectonic shifts that will impact cyberspace and cybersecurity? And specifically, how will policies expand or contract opportunities for countries and regions?

The connected world presents amazing opportunities, but also significant risks, particularly in cybersecurity. But risks are not just from the commonly recognized sources such as criminals, malware, or even targeted cyberattacks; they can emerge from policies as well. Societal responses to immigration challenges, educational and workforce needs, trade liberalization, as well as international cooperation to resolve cyberconflict will shape the future of cyberspace across both developed and emerging economies. Successful policies must balance enabling innovation and advancing cybersecurity.

Cyberspace 2025: Today's Decisions, Tomorrow's Terrain describes projected changes in the online world and the resulting opportunities for collaboration and innovation, as well as the risks of isolation and misplaced regulation. It does not pick winners and losers, but it does allow the reader to evaluate the outcomes of various policy choices across a diverse range of domains—such as education, immigration, and trade—and their implications for cybersecurity.

Today's public policy decisions can address yesterday's problems, or they can shape the future landscape of cyberspace. In some instances, they may even accomplish both aims. The policymaker's dilemma, however, is how to do this consciously. This report gives policymakers, business leaders, and other decision makers a set of scenarios and a framework for evaluating today's policy decisions. Making more data-driven decisions and dedicating resources to support them can create a less daunting and more navigable terrain in cyberspace for 2025 and beyond.

This report is intended to spark dialogue, debate, and more understanding about the challenges and opportunities that lie ahead and ways to benefit from them.

J. Paul Nicholas, Senior Director
Global Security Strategy and Diplomacy
Microsoft Corporation

Understanding Cyberspace in 2025

What will cyberspace look like 25 years into the new millennium? By 2025, more than 91 percent of people in developed countries and nearly 69 percent of those in emerging economies will be using the Internet. Internet dependence will not just be a concept, but rather the new reality.

The future of cyberspace is more than the bigger numbers. The real story involves the character of cyberspace and the implications and impacts that it may have for a country's economic, education, immigration, and trade policies. The relationship between the national policy and cyberspace is complex and, at times, indirect. This report was undertaken to help illuminate these relationships, increase understanding, and support more informed decision-making in both the public and private sector.

This paper presents three scenario-based views of the world in 2025. The scenarios are grounded in an econometric model—the Cyber 2025 Model—that draws upon over 100 socioeconomic indicators. This quantitative analysis is complemented by insights from leading researchers, multilateral institutions such as the World Economic Forum, and other experts on the issues that will affect the world regardless of which scenario comes to fruition.

Several key questions can help frame the future of cyberspace:

- **What are the global mega-trends emerging now that will lead to change over the next decade? How will these trends impact information and communications technology?**
- **Can predictions be accurate enough that policymakers can anticipate how today's choices may lead to different future results?**
- **How might today's policy choices impact cyberspace and cybersecurity?**
- **Can policy structures and frameworks be designed that encourage desirable outcomes and minimize undesirable consequences?**

The force and pace of technological change over the next decade will present challenges and opportunities for individuals, societal organizations, businesses, and governments. One of the primary challenges facing government policymakers is how to balance massive technological change and simultaneously manage the new generation of risks to cybersecurity. The World Economic Forum has identified cybersecurity among its top global risks for the last eight years.[1] Indeed, the same technological advances that present opportunities of economic growth and are shadowed by undesirable consequences.

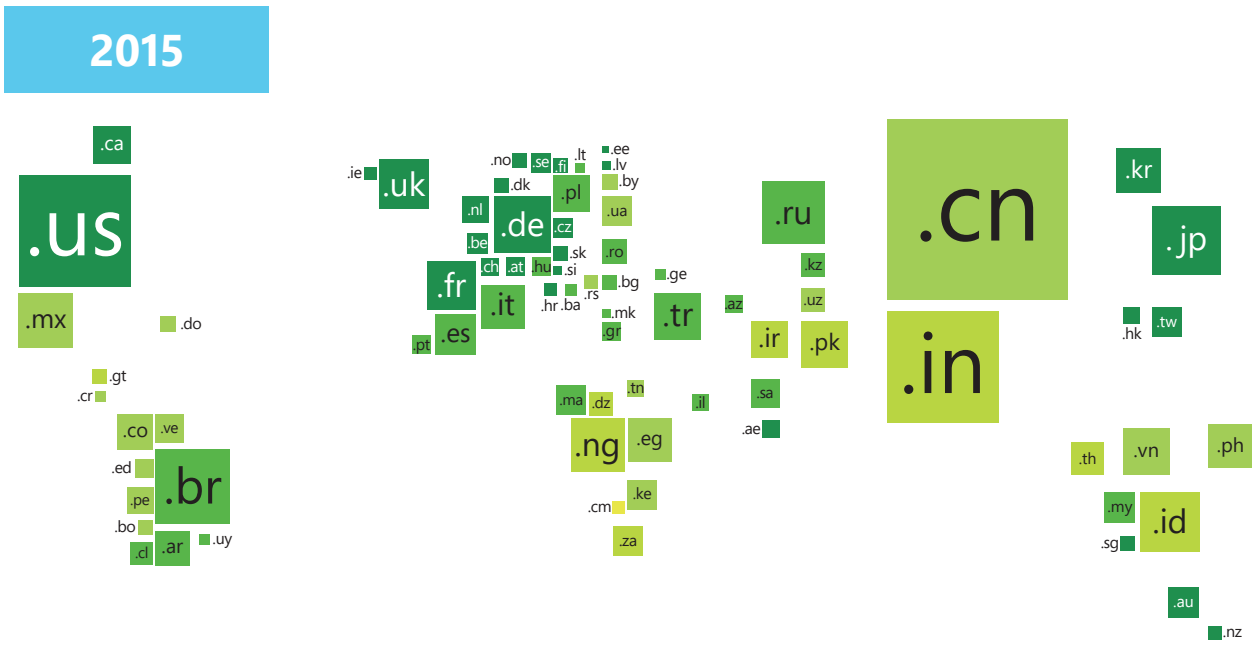
The key to success is preparation and balance. The goals of this paper are to help policymakers, businesses, and societal organizations better prepare for the technological changes ahead; take advantage of information and communications technology (ICT) advancements to address concerns such as governance and socioeconomic well-being; and enable all stakeholders to thoughtfully consider how present-day policy choices might influence future outcomes.

The terrain of cyberspace will be shaped by people and the decisions they make. The objectives and actions of governments, businesses, and societal organizations today will shape the progress of technology in the future. Their policies, programs, and investments can support or undermine ICT development and global cybersecurity. For example:

- Governments can open or restrict trade, allow or prohibit foreign investment, involve or exclude stakeholders in policy discussions, promote or constrict multi-stakeholder collaboration, develop and uphold international standards or create nation-specific standards.
- Businesses can invest in research and development to create transformative technologies, or simply use technology as a means to reduce costs. They can proactively support the development of technology to increase productivity, or they can resist technological change.
- Societal organizations can prepare workforces to meet evolving labor market demands, or they can sustain outdated education and training systems. They can emphasize skills training and digital literacy for all, or accept skills and literacy gaps.

Figure 1: The Cyber 2025 Model: State of Global Internet Adoption in 2015 and 2025

These maps show the distribution of global Internet users in the years 2015 and 2025. The size of each country block (identified by its top-level domain name) conveys the number of Internet users in that country, while the color represents the proportion of Internet users relative to total population. Larger blocks represent countries with more Internet users; darker colors represent countries with a higher percentage of Internet adoption.



Sizing Legend

☐ = 5M Internet Users

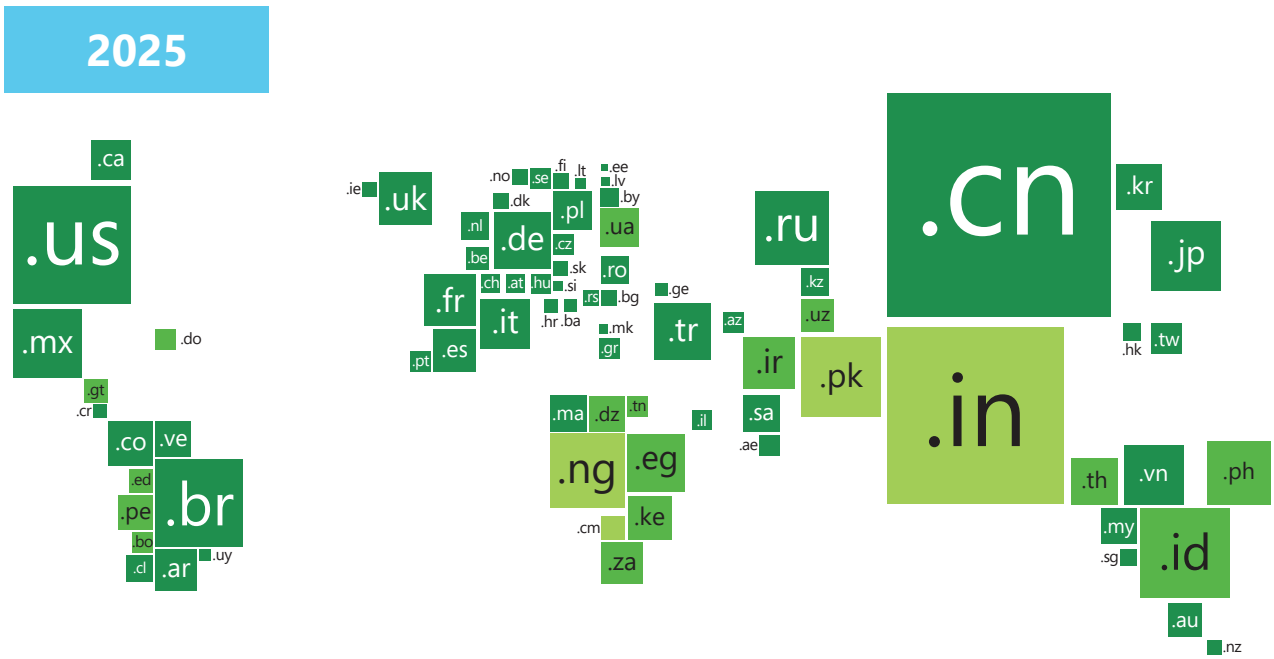
☐ = 10M Internet Users

Percent Penetration of Internet Users

0-20 | 21-40 | 41-60 | 61-80 | 81-100

Number of Internet Users

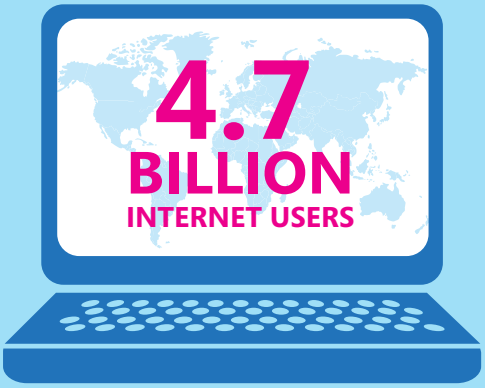
	Brazil	China	France	Germany	India	Japan	Mexico	Nigeria	Russia	USA
2015	127M	751M	54M	72M	283M	109M	68M	66M	90M	287M
2025	173M	1.1B	62M	74M	708M	111M	106M	126M	124M	317M

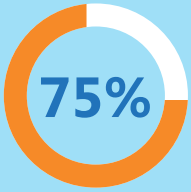


Map concept derived from Geographies of the World's Knowledge, Graham, M., Hale, S.A. and Stephens, M. (Convoco! Edition, London, 2011).

QUANTIFYING THE WORLD IN 2025

HOW MANY INTERNET USERS WILL THERE BE IN 2025?





Percentage from emerging economies

COUNTRIES EXPECTED TO SEE THE GREATEST INCREASE IN INTERNET USERS FROM 2012

CAMEROON 987%

PAKISTAN 631%

GUATEMALA 519%

ALGERIA 385%

WILL THE WORKFORCE KEEP UP WITH THE GROWING DEPENDENCE ON TECHNOLOGY?

ANNUAL STEM GRADUATES

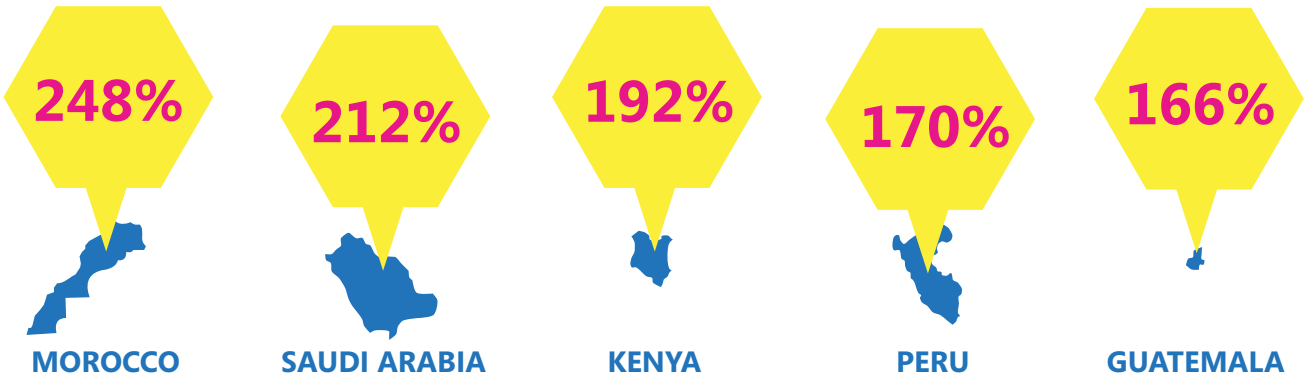
Emerging economies

Developed countries

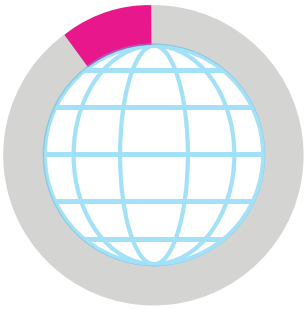
By 2025, emerging economies will produce nearly 16 million graduates in science, technology, engineering, and mathematics (STEM) fields annually, which will be nearly 5 times greater than the 3.3 million per year from developed countries.

COUNTRIES WITH THE STRONGEST GROWTH IN STEM GRADUATES FROM 2013

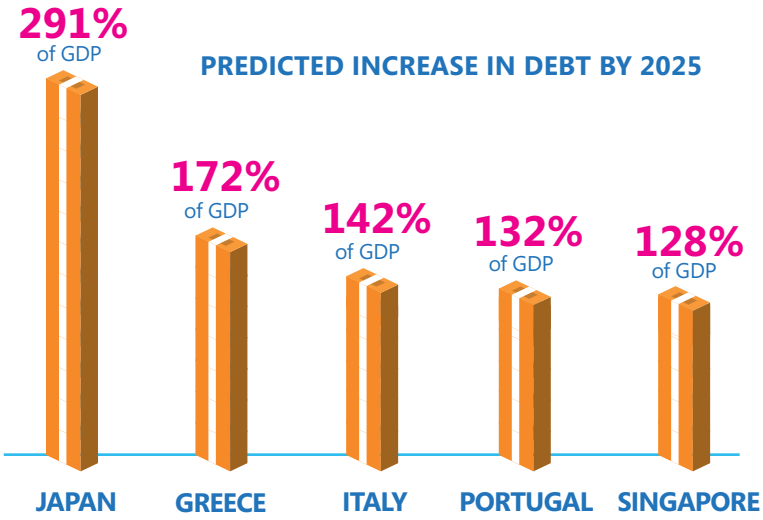
(PERCENTAGE OF GROWTH)



HOW WILL THE WORLD MANAGE GROWING PUBLIC DEBT?

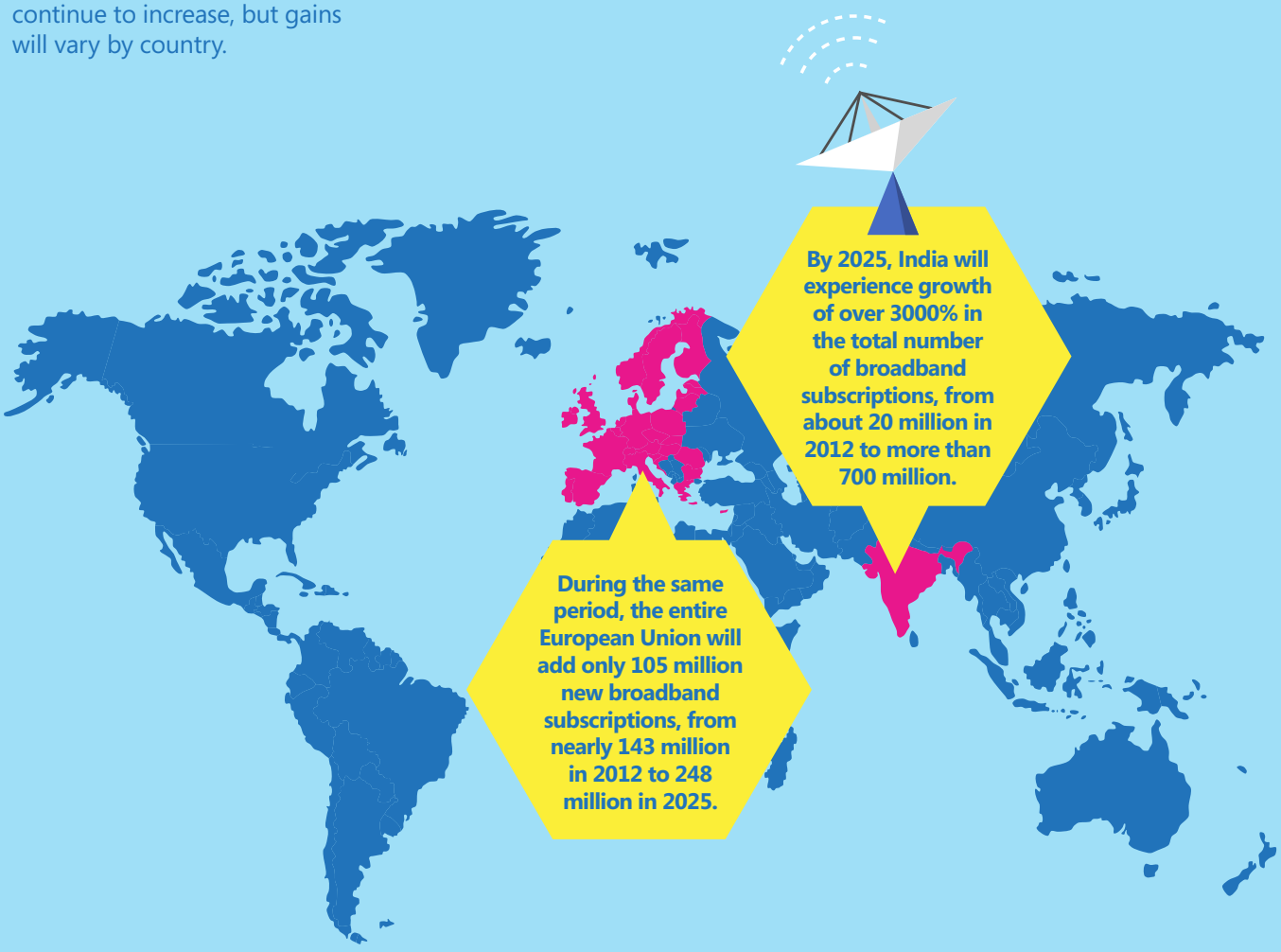


National debt as a percentage of GDP will average just over 10 percent worldwide, but some countries/regions will carry greater debt.



CAN THE WORLD DELIVER CONNECTIVITY FOR EVERYONE?

Broadband penetration will continue to increase, but gains will vary by country.



The Cyber 2025 Model

Methodology

When predicting global futures, a solid foundation in quantitative analysis is critical. The Cyber 2025 Model is rooted in analysis that provides a baseline for potential scenarios that could result from policy choices. Specifically, it builds on historical data of 80 countries from 1990 through 2012 to create 2025 forecasts employing key indicator categories of macroeconomic, socio-demographic, and technology conditions.

The indicators were modeled using two different regression types: linear panel data approach and non-linear S curve approach.[2] More than 100 different potential predictive indicators and thousands of indicator combinations were tested to generate the most statistically significant results.

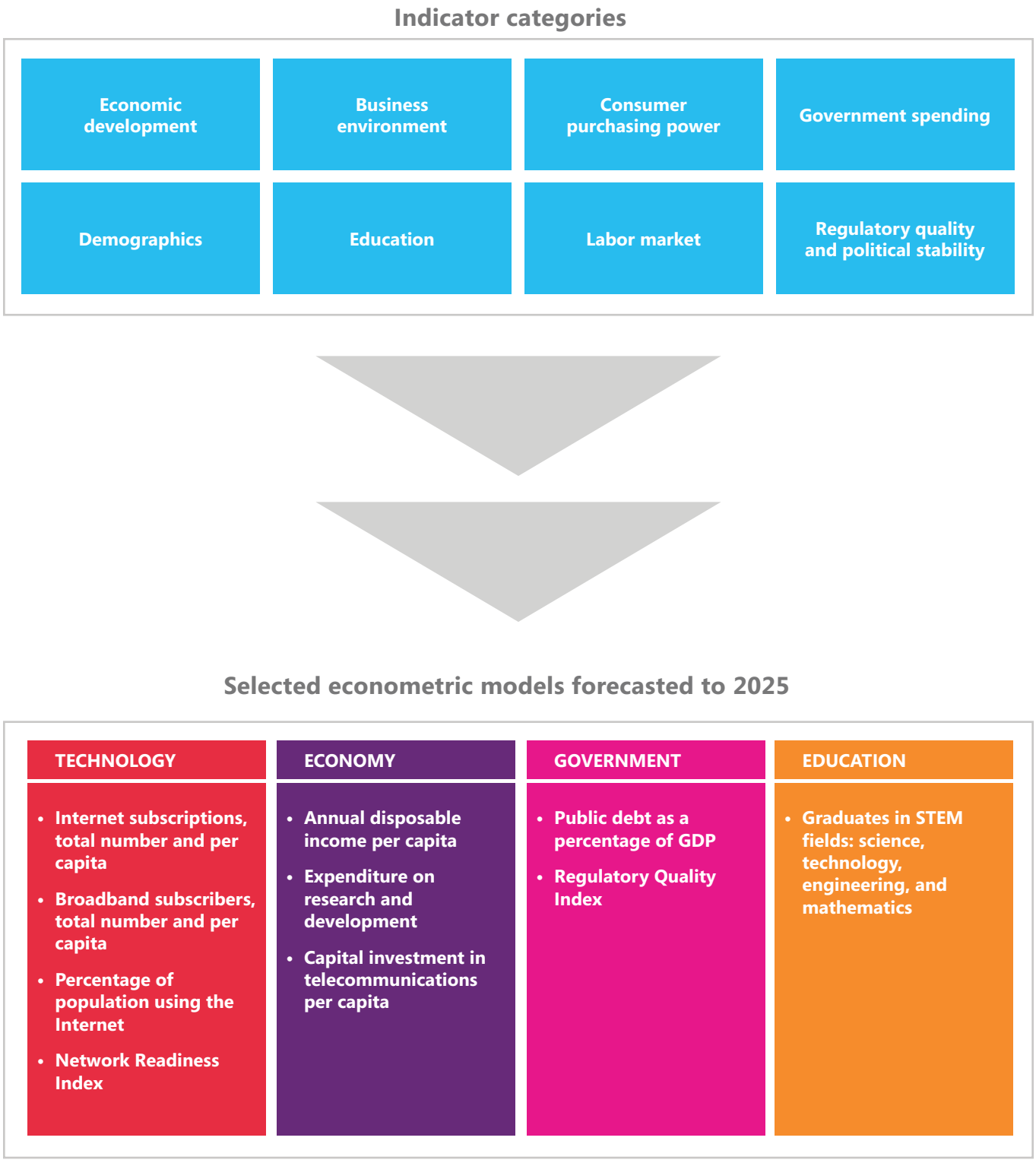
Ultimately, the Cyber 2025 Model delivered several layers of analysis that were woven into the fabric of this paper:

- Baseline forecasts for 80 countries derived from the finalized econometric models
- Optimistic and pessimistic forecasts for each baseline prediction that reflect economically meaningful deviations based on historical country-level fluctuations and long-term trends
- Key predictive indicators that contribute to the development of each model

The baseline, optimistic, and pessimistic forecasts set up realistic underpinnings for each of the three scenarios. Then, each of the 10 models was analyzed to determine the relative strength of its predictive indicators—this meant that the econometric work not only identified indicators that could predict future economic growth, but it could also show which indicators contributed most to that growth.

Building on this foundation of quantitative analysis, additional secondary research was conducted to validate the econometric findings, further shape the scenarios, and explain the key factors influencing the scenarios. This enabled an exploration of qualitative dimensions of the world in 2025. Indeed, both elements—econometric analysis and research-driven insights—were essential to developing the future scenarios. Finally, the research team's knowledge and expertise of the cybersecurity ecosystem helped to place the data into perspective.

Figure 2: *The Cyber 2025 Model: Delivering a Data-Driven View of the Future of Cyberspace*



Future scenarios: Plateau, Peak, and Canyon

PLATEAU

The Plateau scenario is characterized by asymmetry. Political, economic, and societal forces both bolster and hinder technological progress and cybersecurity. Some governments have inconsistent policies and standards with varied levels of stakeholder participation and international cooperation, while other governments form clusters of open trade and foreign direct investment (FDI). Some countries are able to leverage technology to advance economic and socioeconomic development, while other countries are left behind technologically, unable to fulfill the potential of ICT. This fragmented and uneven approach to governance and the economy leads to a less than optimal global cybersecurity landscape.

The Cyber 2025 Model predicts that there will be 4.7 billion Internet users in 2025.

Nearly half of them will come online between 2012 and 2025, almost entirely from emerging economies.

PEAK

The Peak scenario is characterized by clear, effective government policies and standards across economies, and strong collaboration between governments to support open trade and promote FDI. This is a scenario of innovation, in which ICT fulfills its potential to strengthen governance models, economies, and societies. The actions of governments, businesses, and societal organizations foster the widespread and rapid adoption of technology. The political, economic, and social support leads to accelerated economic and technology growth and improved global cybersecurity.

CANYON

The Canyon scenario is characterized by obstructionist government policies and standards, protectionist stances, and isolation. This significantly restricts trade and FDI and undermines relationships across industrial sectors within countries as well as between countries. In this scenario, economic and technology growth is slower, with limited adoption of ICT and deep failures in cybersecurity.

Three future tectonic shifts

The Cyber 2025 Model forecasts that the next 10 years will witness expansive technological growth, significant demographic shifts, and increasing education needs. These trends present three challenges for the future of ICT and cybersecurity:

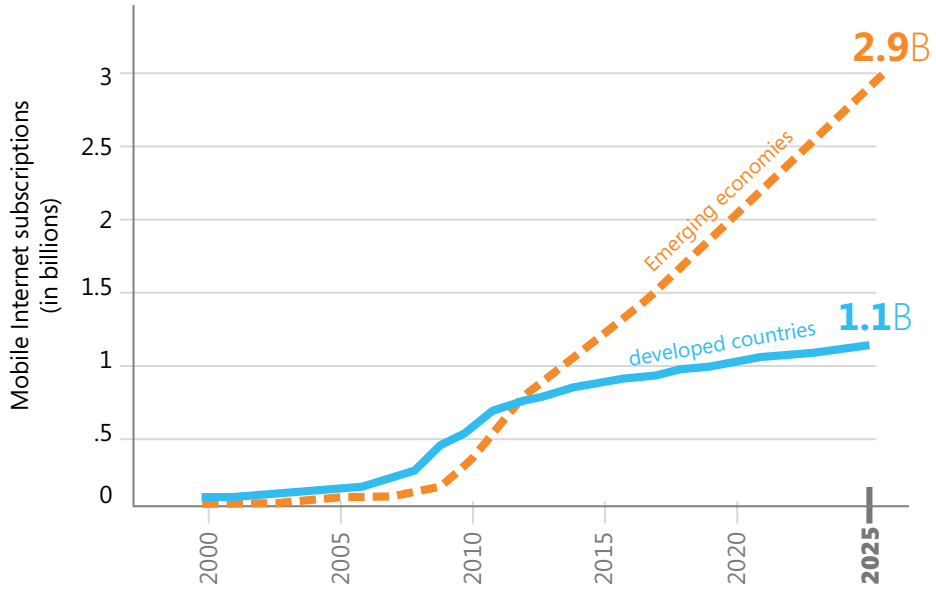
- Realizing the potential of transformative technology while safeguarding against threats to security and privacy
- Addressing the mounting resource needs associated with changing demographics
- Preparing workforces with the skills required to meet evolving needs

To enable understanding of how these trends may develop and their potential impact on cybersecurity, below is a summary of learning from the Cyber 2025 Model that includes research from leading thinkers in academia, government, industry, and such multilateral institutions as the World Economic Forum.

New technology users and growing risks

The adoption of new technology is occurring at a faster rate, and is having a more pervasive impact than ever before, while cybersecurity laws, policies, and even social norms struggle to keep up with new developments. Understanding the growth patterns of technology and the resulting risks will be essential to designing appropriate protections against online threats. *In the Cybersecurity Risk Paradox*[3], a white paper reporting on research on the impact of social, economic, and technological factors on rates of malware, Microsoft found a strong relationship between technology adoption and cybersecurity. In particular, the research revealed that emerging economies are likely to experience an increase in cybersecurity incidents as their technology adoption grows.

Figure 3. ***The Cyber 2025 Model: Mobile Internet Subscriptions 2000–2025***



The extent of this unprecedented pace of technological adoption is perhaps best demonstrated in the rapid market penetration of smartphones. The *MIT Technology Review* compares market penetration of different technologies in the United States since the patent of the telephone in 1876. Whereas landline phones took almost a century to reach market saturation, mobile phones achieved comparable levels in just 20 years. At an even faster speed, smartphones are expected to reach saturation in the U.S. in less than 10 years.[4]

Worldwide, smartphone adoption has grown from less than 1 percent of the world's population in 2007 to almost 10 percent in 2012, a tenfold increase in just five years.[5] If this pace of mobile adoption continues, 80 percent of Internet connections could originate from a mobile device by the year 2025.[6]

The quick adoption of smartphones reflects movement towards an Internet-based society including the Internet of Things, a term that refers to the growing number and variety of physical objects that communicate with each other through the Internet. No longer is the Internet limited to a laptop or smartphone—it increasingly connects previously unconnected devices, leading to cars capable of driving themselves and medical devices that can provide remote, real-time updates to hospitals. Over 50 billion objects are expected to be connected to the Internet by 2020.[7]

The Cyber 2025 Model predicts that by the year 2025, emerging economies will have overtaken developed countries as the larger market for in-home consumer electronics, with emerging economies comprising over 60 percent of the total global market.

The growth of new technologies, such as the Internet of Things, will lead to changes in global consumer trends. The Cyber 2025 Model predicts that by the year 2025, emerging economies will have overtaken developed countries as the larger market for in-home consumer electronics, with emerging economies comprising over 60 percent of the total global market. This shift will require global technology suppliers to adapt their products to these new markets. Market regulators then will need to consider how to attract a combination of global and local suppliers to meet this demand.

Growth in connected devices and overall technology use will accelerate the global trend towards cloud computing. By 2025, most of the data created in the world will move through or be stored in the cloud at some point. Most countries will recognize that cloud technology is not only a necessity for meeting the information demands of their citizens, but also requisite for participation in the global economy. Businesses will lead the adoption of cloud technology in order to remain competitive and efficient. Governments in developed and emerging economies will follow quickly to cut costs, enable services, and mitigate dependencies on legacy equipment.

As the cloud becomes increasingly necessary to the development and delivery of critical services, so too will the desire of some governments to regulate it. Balancing key national interests such as the protection of critical infrastructure and ensuring the security, privacy and reliability of data will become an important topic of debate.

Striking the right balance will enable some countries to reap the benefits of a modern connected state—reduced costs, improved e-government, and increased convenience. Countries that seek to reflexively regulate new technologies without fully understanding how these technologies will impact their economy and culture risk creating burdensome compliance regulations that will ultimately restrict economic innovations in key sectors of their economy domestically and internationally.

Divergent global trends in aging

The Cyber 2025 Model shows two critical demographic shifts expected by 2025—developed countries face rapidly aging populations and falling birthrates, while emerging economies can expect more working-age adults because of rising birthrates. These changes will have a dramatic and lasting effect on resource needs and long-term economic sustainability.[8]

The first shift, aging populations, is especially significant for developed countries. Some of these, like Japan and France, already have disproportionately large populations of older people. This trend will become more prominent in the coming 10 years. One measure of the impact of age on an economy is the dependency ratio, which refers to the percentage of the population younger than age 14 and older than 65—that is, those who are dependent on working adults. The Cyber 2025 Model forecasts that developed countries will move from having one dependent person (child or retiree) per working-age adult in 2012 (a one-to-one ratio) to a three-to-two ratio in 2025.[9] This will be driven by an increase in those over age 65.

According to the Cyber 2025 Model, there will be 850 million people over age 65 in the year 2025, a 60 percent increase over 2012.

Research from the International Monetary Fund indicates that about one-third of the expected increase in public health spending in developed economies over the next 20 years will be attributed to aging populations—roughly 1 percent of aggregate GDP for these economies. (This spending is lower for emerging economies but still significant, and roughly half of health spending growth is projected to come from expenses related to aging.)[10] The situation is aggravated by the fact that while this economic burden is increasing, the number of working-age adults available to carry the burden will be decreasing.

The second demographic shift, an increase of younger populations, is occurring in many emerging economies. The Center for Strategic Studies calls this a "demographic sweet spot," where societies have the opportunity to reap the benefits of a large working-age population brought about by historically high birthrates followed by declining birthrates.[11] That said, this opportunity for growth can be realized only if young people are able to find employment and propel their countries into higher levels of prosperity. In the absence of jobs, these worker-rich communities may fall short of the economic gains that a thriving workforce could make possible.

Demographic shifts will accelerate and drive public policies related to the delivery and protection of ICT services. For example, the rise in older populations could drive increased policy support for telemedicine, different approaches to public safety, and the capacity to address consumer issues that acutely impact older citizens. The growth of younger populations in emerging economies will drive a new cycle of purchasing technology for personal use, in addition to demand for professional technology that will enable collaboration and greater connectivity.

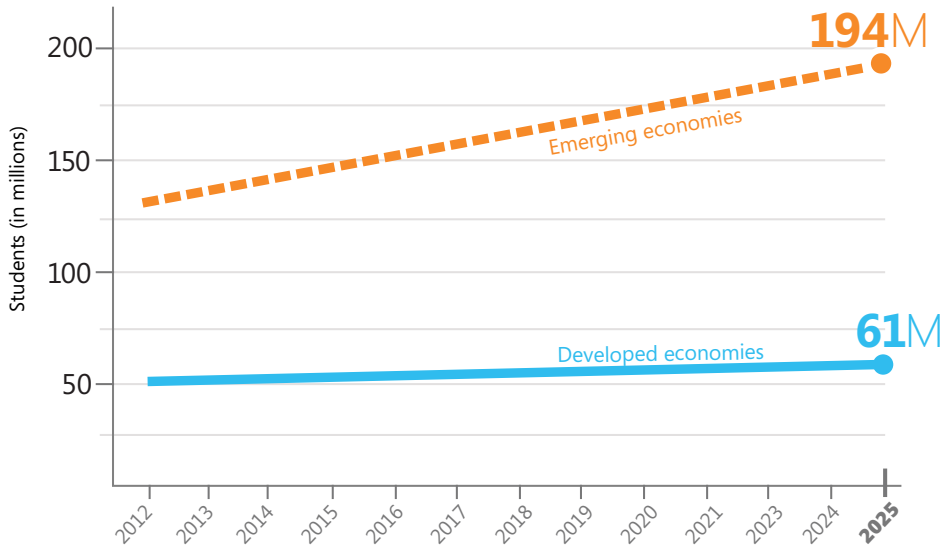
Meeting new human capital needs

The demographic changes described above will profoundly affect how nations use human capital, their most important resource. According to the World Economic Forum (WEF), "Human capital will soon rival—and may even surpass—financial capital as the critical economic engine of the future."[12] The McKinsey Global Institute projects a shortage of 83 to 85 million medium- and high-skilled workers and a surplus of 90 to 95 million low-skilled workers.[13]

The raw numbers show the big picture, but the skills gap can be more specifically defined by the need in developed countries for appropriately skilled workers and the lack of training that aligns with market demand.

First, aging populations in developed countries create a growing need to hire employees from other countries to replenish their workforce. Additionally, businesses are making significant strides in building into their human resources strategies the ability to move skilled employees from one country to another (also referred to as talent mobility). These initiatives will become increasingly important because a greater share of higher-education students will come from emerging and developing countries. The Cyber 2025 Model projects that in 2025 there will be roughly 75 million more students in higher education than there were in 2012.

Figure 4. ***The Cyber 2025 Model: Higher Education Students, 2012–2025***



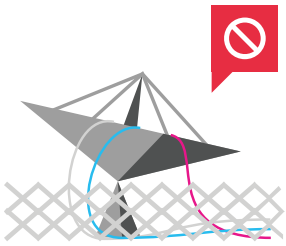
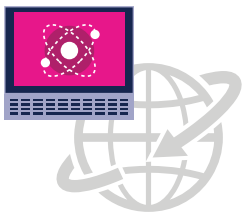
Emerging economies will have about 63 million more students in higher education in 2025 than they did in 2012.

The second feature of the skills gap is that raising education levels alone is not enough to address the problem; the education and training curricula must dovetail with industry needs. For example, there is a growing and unmet need for graduates in science, technology, engineering, and mathematics (STEM fields). The US Bureau of Labor Statistics projects an annual addition of more than 122,000 jobs in computing occupations that require a bachelor's degree in computer science, yet only 51,000 of these degrees are awarded each year. Emerging economies such as China, India, and Brazil demonstrate a different pattern. For example, only 4 percent of bachelor's degrees in the United States are in engineering, compared to 31 percent in China.[14] The imbalance in STEM graduate rates will heighten the need for, and competition surrounding, technical talent and the mobility of that workforce.

The competition for technical talent could increase as countries develop public policies that enable them to grow and attract the talent needed to advance economic and development goals. For businesses and governments, a lack of adequately skilled human capital can severely constrain innovation, growth, and the ability to manage day-to-day activities of an information society. For individuals, unemployment or underemployment has both immediate and long-term effects on income and on socioeconomic conditions. Clearly the number of people relying on ICT will continue to rise, but there is a question about whether there will be a large enough pool of STEM graduates to innovate and secure the ICT services required in 2025.

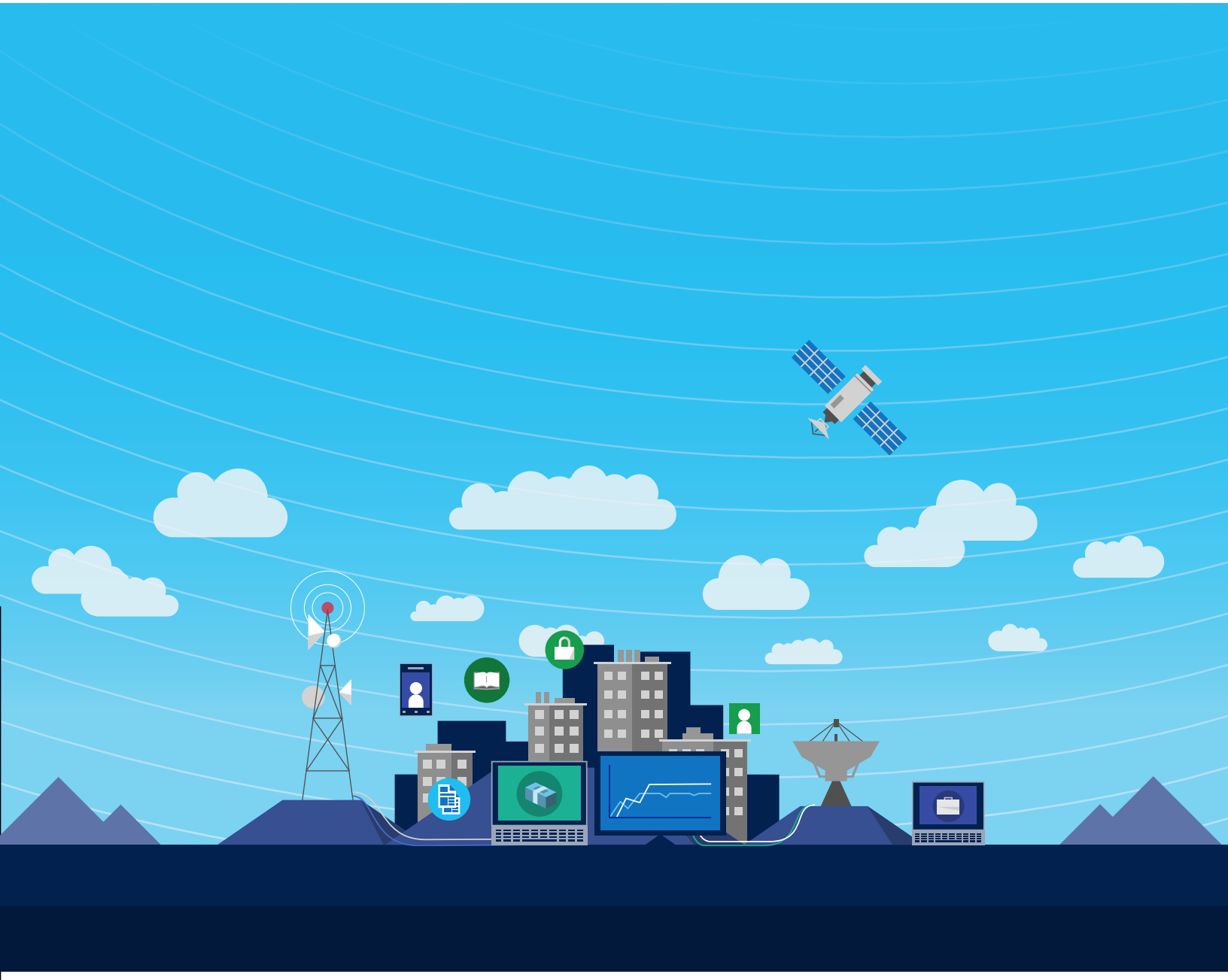
Wild cards: unpredictable factors of change

While the tectonic challenges discussed above are rooted in data and relatively predictable in this horizon, there are additional factors that could dramatically accelerate, slow, or fundamentally change the three scenarios that follow. While they may be difficult to plan for, they should be considered alongside the other factors in this report.

POTENTIAL FOR AN UNFORESEEN EVENT THAT PROFOUNDLY AFFECTS CYBERSPACE	
	The world could experience an event that is random, that computer models could not have predicted, and that creates a major shock or effect. The attacks on the United States in 2001 are an example of just such an event (sometimes referred to as a *black swan event*). Such an event could move countries to implement regulations and controls that could negatively impact technology growth projections and dramatically change the cyberlandscape of the future.
ABSENCE OF CYBERSECURITY NORMS COULD ERODE THE SECURITY AND STABILITY OF THE INTERNET	
	The continued lack of cybersecurity norms emboldens nation-states to exploit the Internet. This could cause the core trust mechanisms of the Internet to be targeted or exploited in an exchange of countermeasures between states. The resulting instability and insecurity could cause the splintering of the Internet, where regions trade global connectivity for regional stability and control.
SIGNIFICANT DISRUPTION IN THE ROLES OF GOVERNMENT AND THE PRIVATE SECTOR	
	The increasing dependency of societies on ICT will require the private sector and government to work together more closely, and in new ways. An unexpected event, such as a catastrophic cyberattack, could lead to a drastic change in the relationship between government and the private sector, such as a government takeover of portions of the ICT industry or the passage of draconian ICT regulation.


PLATEAU
PEAK
CANYON

PLATEAU: Stable but Stalled



PLATEAU

In the Plateau scenario, some countries and regions benefit from support from governments, businesses, and societal organizations for ICT development, while other countries and regions present an environment that is less hospitable to ICT growth. The baseline forecast created by the Cyber 2025 Model for this scenario is marked by uneven technological growth and advancement—some countries use technology to positively transform their societies while others struggle to overcome obstacles.

What are the implications of a scenario with such disparate outcomes from country to country? What is the result of adding the tectonic shifts in technological growth, demographic changes, and workforce imbalances to a future world that extends many of today's imbalances?

KEY CHARACTERISTICS	IMPACT ON TECHNOLOGY AND ECONOMIC DEVELOPMENT	CYBERSECURITY OUTLOOK
• Inconsistent government policies and standards • Examples of cooperation in some areas but not others • Clusters of open trade and liberal rules for foreign direct investment, while other countries and regions remain closed • Varied levels of stakeholder participation and international cooperation	• Economic and technology growth differ dramatically from country to country. • ICT development is supported in some countries and industries and not others.	• Societies struggle with security challenges, as responses are often limited to individual nations or sectors despite the trans-border nature of Internet infrastructure. • Government focus is often on compliance over security.

PLATEAU FORECASTS BY THE NUMBERS

R&D investment in developed countries grows only **25 percent** between **2012** and **2025**, while the R&D investment of emerging economies **more than doubles** during the same period.

By **2025**, emerging economies experience a **sixfold increase** in **broadband penetration rates**, but still lag behind the penetration rate in developed countries.

Annual disposable income per capita grows **65 percent** in emerging economies, but even these impressive gains are approximately **10 percent** less than in the Peak outcome.

Governments both embrace and restrict ICT development

Like today, some Plateau governments have effective policies supporting long-term economic development. They embrace open trade and stimulate a dynamic private sector, while other governments limit trade and distort markets. These varied government approaches are apparent in the Cyber 2025 Model, where regulatory quality varies considerably by country and region. Some governments effectively stimulate private sector development, while others do not, ultimately undermining their economic growth.

In the Plateau scenario, ICT policies also vary by country. Some countries eliminate barriers to digital trade, whereas others erect them. Intellectual property is staunchly protected in some countries, while others deny, revoke, or invalidate patents and intellectual property (IP) rights. The world divides into blocs that adopt policies that enable ICT growth and development, and blocs that create an uncertain business environment for technology innovations. Clusters of cooperation exist, but many countries that seek to control information and trade work bilaterally. In sum, globalization and trade continue, even as certain policies impede growth.[15]

Even though some Plateau countries use technology to advance economic and social development, their ability to continue that advancement is at risk. When too many countries choose not to engage in international dialogue or develop positions that are inherently incompatible with the advancement of global ICT, international efforts are weakened, and opportunities to benefit from a global marketplace are hindered.

Business, economic, and ICT development growth is uneven

The Cyber 2025 Model reveals highly uneven growth in Plateau economies, which can be linked to disparate national polices. Free-trading countries with cohesive policies promote long-term economic development and good governance. On the other hand, protectionist countries with disjointed policies experience volatile economic conditions.

The uneven growth among countries and uneven distribution of that growth within them affects access to ICT. The Plateau scenario suffers from a digital divide much like today's, with two types of world citizens as described by the World Economic Forum: "One empowered by access to [ICT] to improve their own livelihood; the other stunted and disenfranchised by the lack of access to ICT that provide[s] critical development opportunities."[16]

The uneven growth among countries and uneven distribution of that growth within them affects access to ICT. The Plateau scenario suffers from a digital divide much like today's.

In the Plateau scenario, even those enterprises benefiting from favorable domestic business environments at home miss the opportunity for greater returns abroad. They may be willing to expand internationally, but protectionist regimes block access to these markets, which over time constrains Internet use and limits innovation.

Differing approaches to ICT lead to contrasting social conditions

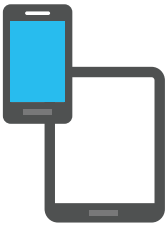
In the Plateau scenario, many countries start planning for their aging (or youthful) future populations early. Technology plays a critical part in helping them navigate these demographic transformations.

Other countries are not as proactive. The Cyber 2025 Model illustrates the tremendous impact of the failure to address aging populations: the population aged 65 and up is the leading indicator of public debt by a very large margin. The failure to prepare for these expected demographic shifts therefore has serious consequences. Aging populations in these unprepared Plateau countries produce unmanageable public debt increases, while growth of the youth population can lead to unemployment crises and social instability.

Plateau countries also respond to the evolving workforce in varied ways. Those that leverage the potential of ICT and encourage cooperation across industrial sectors such as health, finance, and manufacturing see increased talent mobility and flexibility as well as effective education and skills training. Other countries have governments that do not reach out to societal organizations or to businesses to learn about market needs or to coordinate education and skills training efforts. These disparate approaches hinder even those countries that proactively prepare for demographic shifts, as they have a smaller global pool of well-trained workers from which to draw.

Cybersecurity characteristics of the Plateau scenario

TECHNOLOGY FOUNDATIONS



- Mobile devices become the common means for Internet access in both developed and emerging economies, which encourages new mobile devices and services that further leverage cloud computing. However, incongruous and fragmented compliance and regulatory requirements may limit the growth of new companies.
- Mobile payments will give emerging economies a potential leadership edge over developed countries by encouraging the development of an accessible, secure, and reliable means for individuals to remit money locally and internationally. Governments in emerging economies will increasingly see mobile technology as a way to expand financial inclusion for growing populations.

THREAT ENVIRONMENT

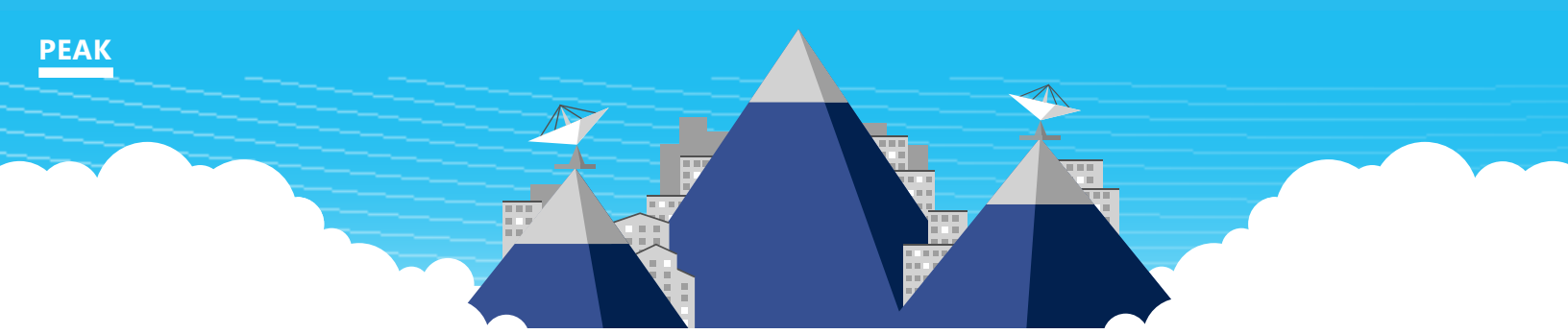
- Online threats affect the full spectrum of ICT users from the highly advanced to the newly connected. Attackers exploit inconsistent security policies and compliance frameworks that were created to enhance security but have resulted in systems that are difficult to administer and defend.
- For developed countries, the threat landscape can result in regular and pervasive data breaches, which in turn can lead to reactive regulatory attempts to improve data protection. In emerging economies, the broad scope of threats coupled with stagnating employment could prompt unemployed computer-trained individuals to shift to cybercrime. Some of these individuals will be recruited by local and transnational organized crime groups, and possibly even nation-states.

GLOBAL COOPERATION

- Many countries, particularly those with emerging economies, will put cybersecurity on par with other intelligence and defense priorities. As more critical public and private information systems move to the cloud, governments will direct additional resources towards defending these systems.
- Increasing levels of cybercrime within emerging economies will compel the governments of these countries to build cybersecurity capacity. Governments may be tempted to abandon international cybersecurity cooperation in favor of more ad hoc processes to meet their short-term needs.
- In some instances, existing forums, such as the Association of Southeast Asian Nations (ASEAN), BRICS countries (Brazil, Russia, India, China, and South Africa), and the Gulf Cooperation Council (GCC), will champion cybersecurity solutions for their own members. These islands of cooperation may hinder adequate responses to global events.

EDUCATION	
	• The majority of higher-education students will come from emerging economies, which will increase the ability of those countries to innovate and create economic opportunities. • Developed economies will experience a widening skills gap even as their dependency on ICT increases, creating challenges for sustaining innovation. The resulting STEM skills gap will cause significant economic and operational challenges, and will force these countries in the midst of mounting public debt to make difficult trade-offs in entitlements to ensure future economic growth.
TALENT MOBILITY	
	• High migration rates of specialized labor to developed countries will contribute to a "brain drain" from emerging economies when this talented labor is most needed for their own economic development. • While developed countries continue to attract talent in the short term, inflexible immigration policies and mounting debt may inhibit long-term competition for talent. Conversely, the growth in talent in emerging economies may not translate into innovation and growth in the short term, but over the long term emerging economies will win in talent retention.
TRADE	
	• International trade policies both advance and constrain cybersecurity improvements; some governments will fear the potential security downsides of technological growth and limit trade, while others will seek maximum access to cutting-edge security technologies. • International trade negotiations will proceed in fits and starts, with cybersecurity incidents portrayed as a basis for either progress or delay, depending on government perspectives.

PEAK: Connected and Cooperative



The most promising global outcome for 2025—the Peak scenario—is characterized by expansive access to technology in most economies. Strong cooperation among national governments as well as between governments and their stakeholders makes this outcome possible. In the Peak scenario, countries accelerate and deepen their transition towards knowledge-based economies with an educated workforce, while governments, enterprises, and private individuals reap the benefits of technology-driven growth.

In this scenario, governance, economic development, and social conditions improve in both developed and emerging economies, although the Cyber 2025 Model shows that emerging economies improve the most. Their regulatory quality improves markedly, their economies grow at faster rates, and ICT development approaches the level of progress seen in developed countries.

In the Peak scenario, the Cyber 2025 Model shows that the regulatory quality in emerging economies improves markedly. In addition, their economies grow at faster rates, and ICT development makes gains approaching the levels in developed countries.

KEY CHARACTERISTICS	IMPACT ON TECHNOLOGY AND ECONOMIC DEVELOPMENT	CYBERSECURITY OUTLOOK
• Clear, effective government policies and standards • Strong international and cross-sector relationships • Open trade and promotion of foreign direct investment • Multistakeholder and intergovernmental collaboration • Ability to attract and retain skilled workers to grow the economy	• Accelerated economic and technology growth • Political, economic, and social support of ICT development	Society experiences the benefits of ICT with improved cybersecurity as a result of continual innovation and collaboration across industrial sectors and international borders.

PEAK FORECASTS BY THE NUMBERS

By **2025**, broadband penetration rates nearly equalize between developed and emerging economies.

Emerging economies overtake developed countries in their capital investment in telecommunications by a margin of **$160 billion** to **$153 billion**.

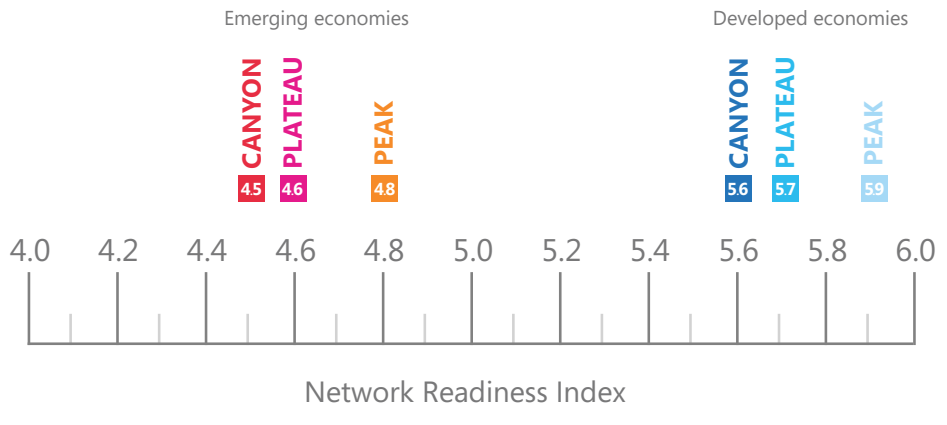
In Brazil, Russia, India, and China (BRIC countries), the annual disposable income per capita doubles between **2012** and **2025**, from **US$3,085** to nearly **US$6,400**.

Governments support ICT development

National policies foster clarity and transparency

In the Peak scenario, national policies foster the favorable business conditions needed to promote economic and technological growth. Countries enable growth in the ICT industry through clear policies that are based on global standards and that are reviewed regularly in light of new developments. Close collaboration with other stakeholders, including those in the private sector, societal organizations, and other governments, strengthens public policies and the ability of governments to leverage ICT and enhance cybersecurity.

Figure 5. ***The Cyber 2025 Model: Projecting the Network Readiness Index in 2025***



The Network Readiness Index of the World Economic Forum measures the readiness of an economy to take advantage of the benefits that ICT offers. The higher the score, the greater the readiness.

The success of technology and infrastructure in emerging economies greatly depends on government action in particular. A study from the University of Redlands in California shows that in emerging economies, foreign direct investment and government support of ICT have the greatest influence on technology use, expenditure, and infrastructure. In the Peak scenario, the governments of emerging economies enable both international and domestic firms to participate in a free and competitive marketplace, especially in innovative sectors like technology. The Cyber 2025 Model projections of the Regulatory Quality Index (RQI) further support the findings of the study, with emerging economies improving their average RQI score considerably in the Peak forecast for 2025.

Most Peak governments keep up with the rapidly evolving technology environment by regularly clarifying their roles in the cyberecosystem, reviewing their policies to ensure relevance and effectiveness, and updating their own ICT systems. Policymakers not only understand the economic benefits of a robust technology sector, but also take advantage of ICT to improve the efficiency, transparency, and accountability of governance.

Peak governments are able to adapt quickly to ICT developments because they work closely with businesses and societal organizations when they develop policies and standards. The importance of this multistakeholder participation was highlighted in 2012 by the *Government Information Quarterly*, which discussed how ICT tools can create "dynamically participative governance models." In the Peak scenario, scientific and business communities, societal organizations, and citizen groups "drive the emergence of ICT applications to exploit the full value of the mass collaboration and the technological developments and governance directions." [17]

Countries harmonize international agreements and standards

Individual countries in the Peak scenario work to harmonize their efforts and to develop the international agreements and global standards that create an environment friendly to the growth of ICT.

International agreements to lower trade barriers are critical for the development of ICT-related trade. For example, the World Trade Organization Information Technology Agreement (ITA) requires participants to eliminate tariffs on a list of ICT products.[18] At present, there has been substantial resistance from some countries to renegotiating the ITA to include ICT products created since the agreement took effect in 1997. Some parties fear that additional products could include those they consider sensitive politically or economically.[19] In the Peak scenario, an updated ITA list provides significantly expanded coverage of ICT products over the current list, with the aim of reducing barriers to accessing ICT products, including those that enable security.

While the Cyber 2025 Model forecasts high economic growth for the Peak scenario, achieving this growth depends in part on the willingness of governments to use global ICT standards and to cooperate in regularly updating them. The Center for Technology at the Brookings Institution asserts that the use of different national technical standards fragments the market, limiting the ability of ICT producers to export on a global scale. Removing the costs and hurdles associated with nation-specific standards "dramatically increase[s] innovation by providing a global platform on which to build." [20] In the Peak scenario, this includes eliminating tariffs and lowering other barriers to trade, including conflicting national standards.

Global cybersecurity standards are especially critical for success. Peak countries jointly identify their ICT security needs and develop processes to verify that those needs are met, without regard to the product's country of origin or where the verification took place. Mutual acceptance of a foreign entity's statement that those needs have been met are the norm in the Peak scenario. While this kind of mutual recognition was pioneered during an era when software was sold as a boxed product, there are new efforts to bring similar levels of assurance to online services. For example, the Cloud Security Alliance

has developed a Security, Trust, and Assurance Registry (STAR) that aims to provide transparency into the security controls that cloud service providers use.[21]

The international standards used in the Peak scenario are supported by inter-governmental collaboration. Regional organizations help facilitate this exchange and provide a platform for policymakers to tailor global standards to region-specific needs. This is particularly important for emerging economies, which face considerable challenges in harnessing the benefits of global standards. The Asia-Pacific Economic Cooperation Telecommunications and Communications (APECTEL) Working Group is a present-day example of a regional organization that supports ICT policy development and strategies. Similar Peak organizations allow government leaders to share concerns, refine standards, and exchange ideas to encourage trade, technological progress, and the application of ICT to socioeconomic development.

Accelerated ICT development promotes business and economic growth

ICT adoption stimulates growth

Thanks to effective national policies and cooperation across industrial sectors, national economies in the Peak scenario experience significant economic growth that is further accelerated by the widespread adoption of ICT. Increasing demand for ICT then stimulates investment in technology expansion and innovation. This in turn boosts the availability of new ICT applications, driving additional demand from consumers and business.

One of the most important Peak features is the extensive use and deep market penetration of mobile computing. While the Cyber 2025 Model predicts mobile Internet subscriptions will increase in all three Cyber 2025 scenarios, in the Peak scenario mobile Internet subscriptions increase by 60 percent in developed countries and by a dramatic 400 percent in emerging economies.

The economic effect of nearly universal access to technology in the Peak scenario is profound, especially for emerging economies. They have greater access to technology applications, and use this increased connectivity to access business opportunities in other countries while growing their own economies.[22]

Technological sophistication multiplies economic and human development opportunities, which in turn create opportunities for technological development.

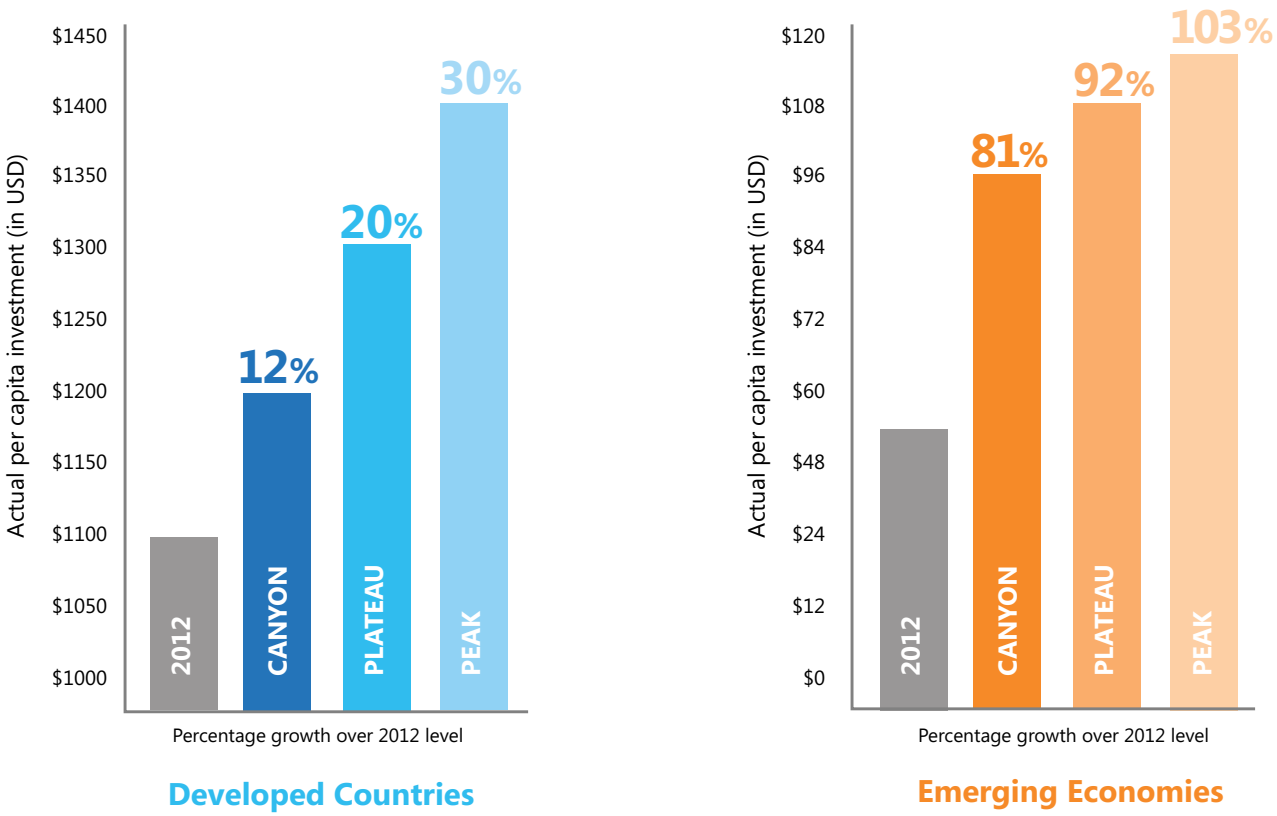
Dirk Swart, *Africa's Technology Futures*, 2011

R&D investments fuel innovation

The strong economic conditions in the Peak scenario create favorable environments for investment in research and development, which drive further economic growth by creating business opportunities and increasing productivity.

Developed countries continue to lead the way when it comes to dollars invested in research and development (R&D), but open trade allows these investments to positively impact emerging markets as well.

Figure 6. ***The Cyber 2025 Model: Projecting Growth in R&D Investment over 2012 Levels***



ICT helps mitigate demographic challenges

ICT assists aging populations

The Cyber 2025 Model suggests that aging populations in developed countries and younger populations in emerging economies can pose significant challenges. Peak countries respond effectively to these challenges by leveraging ICT to enable improvement in major areas of concern, such as healthcare.[23] There, developed countries will face rising total costs, while emerging economies may lack medical professionals to serve their growing populations.

For example, smartphones and other mobile devices are used to improve patient care in both developed and emerging economies. This requires affordable and reliable access to secure ICT infrastructure as well as entrepreneurs focused on medical solutions.

In developed countries, this mitigates costs by providing just-in-time access to services and increasing access to specialist providers. ICT applications currently being tested in developed countries include a stroke recovery app with game-based rehabilitation exercises, and therapies tailored to patients with Alzheimer's, dementia, and long-term illnesses that cause muscle deterioration. Patients can complete these activities at home rather than in healthcare facilities, which reduces the cost.[24] In emerging economies, mobile apps can help provide basic diagnoses, testing, and patient support that is both timely and cost-efficient.

ICT helps prepare workforces for future labor markets

In the Peak scenario, policymakers set educational priorities that expand access to education, improve educational quality, and tailor skills development to market needs. Peak governments work closely with businesses and societal organizations to address the gap between the skills needed to drive economic growth and existing workforce talent.

Access to and adoption of ICT are both driven by and contribute to educational development. ICT can be used for lower-cost education and training, such as with remote training and supervision, which enables students to become trained workers without being in the same physical place as their educators.[25]

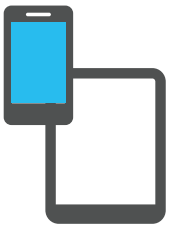
In the Peak scenario, systems are designed to align with specific industry needs and match post-graduate job opportunities. Noting the fluctuating demands of local and national industries over time, the Organization for Economic Cooperation and Development (OECD) states that there is "no 'right' proportion of certain education qualifications in specific occupations."[26] In addition to formal education systems, governments, businesses, and societal organizations collaborate to ensure that workforces are ready for those changing needs, building in skills training to prepare people for the demands of specific jobs.

The Cyber 2025 Model indicates that in emerging economies, adult literacy is the primary socioeconomic driver of growth in mobile Internet adoption.

Cybersecurity characteristics of the Peak scenario

The Peak scenario is marked by a cycle of economic growth and continued ICT development. The growing knowledge-based economy relies on a secure and stable Internet and thus places a premium on security.

TECHNOLOGY FOUNDATIONS



- The Peak scenario is marked by a cycle of economic growth and continued ICT development. The growing knowledge-based economy relies on a secure and stable Internet and thus places a premium on security.
- ICT providers respond to this demand by creating and delivering secure information services and devices. The strong cybersecurity posture in the Peak scenario further accelerates this cycle by instilling confidence in government and the private sector.
- Developed countries in particular will increasingly integrate cloud computing solutions into the core operations of critical infrastructures. Countries will adapt their risk management activities to balance this technology evolution against traditional audit and certification regimes.

THREAT ENVIRONMENT

- Countries in the Peak scenario face a range of attacks, from highly targeted and sophisticated to simple.
  - The principle threat scenarios for developed countries —with new technologies, solid cybersecurity skills, and strong international collaboration mechanisms— include sophisticated, well-resourced organized criminal entities, determined adversaries, and fraudsters that seek to profit from low-end attacks against a large number of people.
  - Emerging economies face many of the same threats, but the proportions are different. For example, they will have a wider range of low-end attacks targeting the growing disposable income of their newly connected citizenry, while the high-end sophisticated threats will be more limited due in part to the lack of key espionage targets such as R&D.
- Both developed and emerging economies are better able to address cyberthreats due to better skills, strong emphasis on collaboration (domestically and internationally), and the deployment of technology that can resist attack.

GLOBAL COOPERATION

- Government and private stakeholders are well prepared to deal with the complexities of responding to fewer cybersecurity incidents. Responders are able to seamlessly mobilize across organizations, industrial sectors, and national borders to contain and mitigate attacks that may span physical, mobile, and cloud-based infrastructures.
- Recognizing the importance of cybersecurity, countries build national cybersecurity strategies that enhance information-sharing and law enforcement cooperation. Concerns regarding civil rights and civil liberties are managed through transparent and cooperative public-private partnerships. Internationally agreed-upon cybersecurity norms and trust among developed and emerging economies contribute to greater stability and security of core Internet functions.

EDUCATION

- Both developed and emerging economies create the right mix of incentives for educational institutions and students alike. The resulting enrollment expansion creates a positive cycle of increased R&D funding for schools. The increased innovation in turn fuels interest for future students and the advancement of technologies in the economy.
- Developed countries continue to invest more in R&D over the long term. Open trade in the Peak scenario enables emerging economies to leverage and share in the benefits of these investments.

TALENT MOBILITY

- The free flow of people and ideas enables the efficient alignment between industry needs and talent resources. Developed countries succeed when they can balance flexible immigration policy and educational incentives to attract, grow, and retain talent over the long term. Emerging economies succeed when they can foster expanding economies, improved educational institutions, and diverse economic opportunities.
- Despite significant increases in the annual number of STEM graduates, the ICT sector may still generate technical jobs at a rate that cannot be matched by available talent because global consumption of ICT is so high.

TRADE

- Liberalized trade enables improvements in cybersecurity by creating an efficient global market for modern devices and services that leverage the latest security technologies.
- International trade negotiations encourage cybersecurity by continually opening markets and reducing tariff and non-tariff barriers to trade, including barriers that may have been portrayed as security-related.

CANYON: Deepening Isolation

The Canyon scenario is characterized by a failure to fulfill the potential of technology to positively transform governments, economies, and societies. Countries are isolated by protectionist economic policies and government resistance to the rapidly changing technological environment. Instead of taking advantage of anticipated ICT growth, governments restrict technology trade and the flow of information. Countries are thus unable to leverage technology to prepare for changes in demographics and labor market needs. While the Cyber 2025 Model illustrates significantly less growth across developed and emerging markets in the Canyon scenario, it is clear that emerging markets have the largest opportunity cost—and the most to lose.

KEY CHARACTERISTICS	IMPACT ON TECHNOLOGY AND ECONOMIC DEVELOPMENT	CYBERSECURITY OUTLOOK
• Unclear, ineffective government policies and standards • Protectionism inhibits cooperation • Significant restrictions on trade and foreign direct investment • Obstructive dynamics undermine internal and cross-country relationships	• Economic and technology growth is slow; wide variance across countries results in extreme instability • Limited breadth of ICT adoption	ICT adoption grows, but society is unable to fully benefit because of the unchecked growth of threats coupled with inadequate responses. Security approaches are overly prescriptive and often nationalistic, and do not respond adequately to changing technology or threat conditions.

CANYON FORECASTS BY THE NUMBERS

In emerging economies, investment in R&D between **2012** and **2025** is **20 percent** of what could be achieved in the Peak scenario.

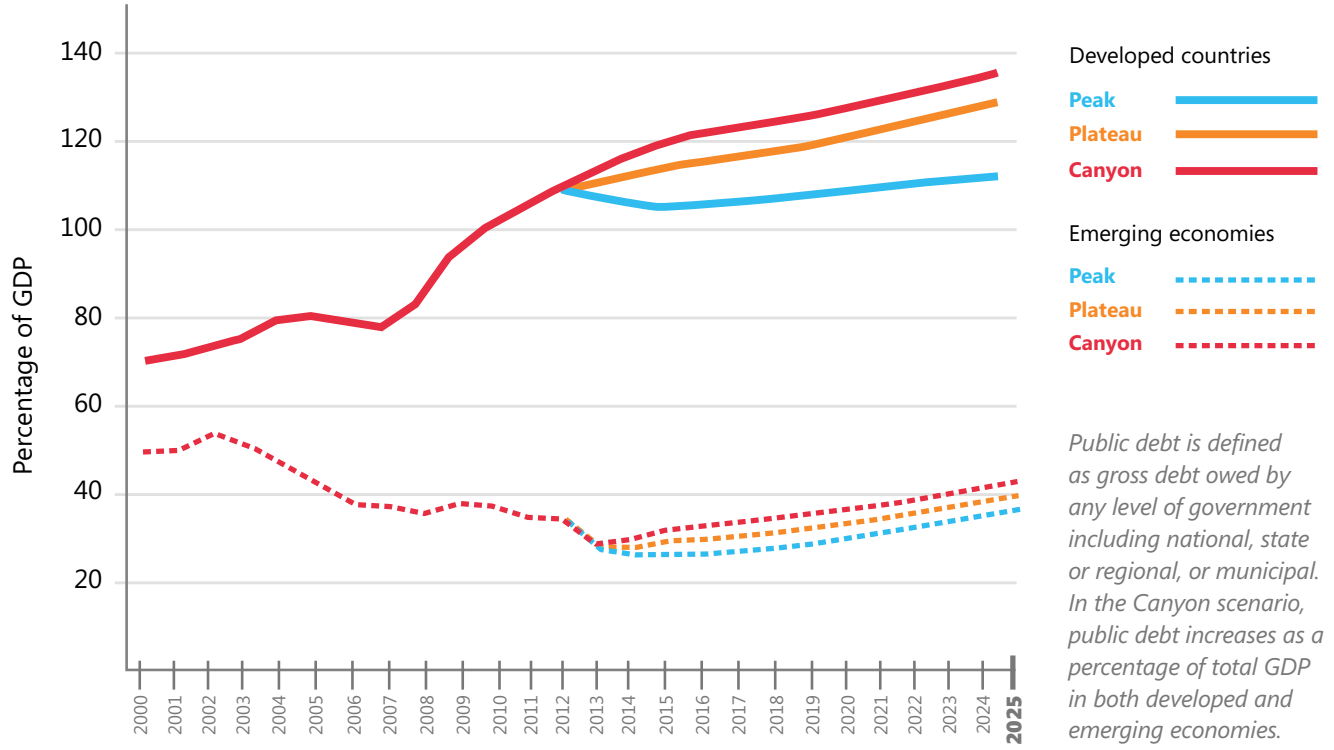
In developed countries, growth in annual income per capita between **2012** and **2025** is **10 percent**, only half of what could be achieved in the Peak scenario.

Governments undermine ICT development

Public debt and low government productivity reduce the use of ICT

The Cyber 2025 Model forecasts a rise in public debt in 2025 in the Canyon scenario, a situation aggravated by failures in government productivity. The gap between public and private sector productivity has been widening for the past 25 years and continues to do so in the Canyon scenario, due largely to government "inability to dynamically absorb and capitalize on new technologies like we've seen in the private sector."[27]

Figure 7. ***The Cyber 2025 Model: Public Debt as a Percentage of Total GDP, 1991–2025***



Public debt is defined as gross debt owed by any level of government including national, state or regional, or municipal. In the Canyon scenario, public debt increases as a percentage of total GDP in both developed and emerging economies.

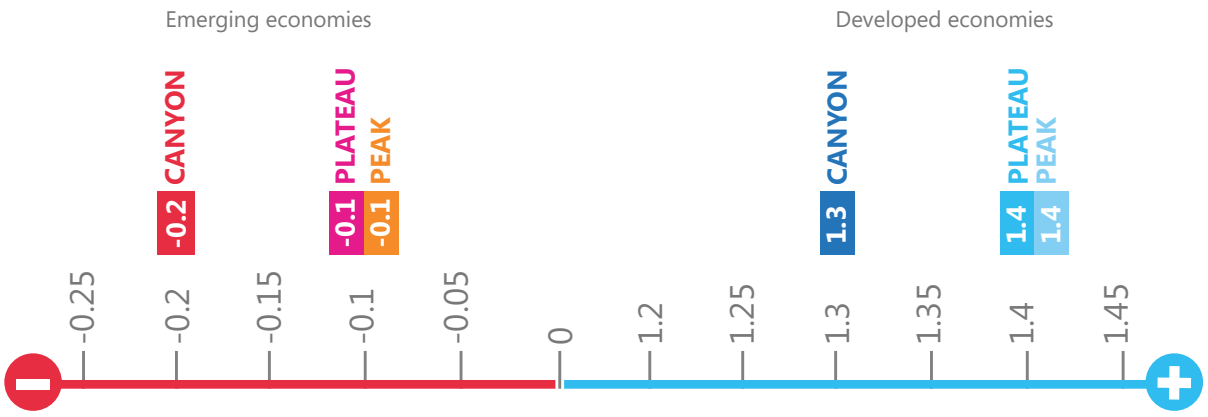
While the private sector in the Canyon scenario is not able to fully leverage the transformative potential of ICT, it nonetheless does what it can. One major factor limiting the private sector's opportunities is government policies. Instead of taking advantage of technology to improve governance and service delivery, Canyon governments restrict the flow of information; use ICT for military purposes and to spy on people, organizations, and other governments; and create bureaucratic and regulatory obstacles that prevent legacy information systems from being updated.[28]

Privacy and intellectual property rights are greatly diminished in the Canyon scenario, leading to a loss of trust in technology. National policies center on controlling ICT systems and create environments unsupportive of research and development (R&D), such as by failing to protect intellectual property or even violating it outright. As a result, private-sector spending on R&D and innovation plummets because individuals and businesses are unwilling to invest in developing technologies that may be pirated or misappropriated.[29]

Short-sighted policies obstruct development

Obstructive policies in Canyon countries stymie private sector development and technological progress. Many of these may have been set as well-intended responses to the sociopolitical pressures placed on national leaders, but by 2025 their negative effects have compounded, to the detriment of both national and global economies. The Cyber 2025 Model demonstrates that emerging economies in particular are deprived of tremendous growth opportunities.

Figure 8. ***The Cyber 2025 Model: Projecting the Future of the Regulatory Quality Index***



The Regulatory Quality Index, created by the World Economic Forum, captures perceptions of a government's ability to formulate and implement sound policies and regulations that permit and promote private sector development. Higher values correspond with better governance.

In the Canyon scenario, economic development policies are "measures designed to protect, favor, or stimulate one country's domestic industries, service providers, or intellectual property (IP) at the expense of other countries' goods and services."[30] These may be intended to bolster national industries or firms, or they may be grounded in valid security concerns. However, favoring domestic firms or restricting market access for foreign competition often suppresses the vitality of the private sector and disrupts the global ICT trade.

Canyon governments also implement protectionist trade policies that disadvantage foreign firms and impede technological development. Billions of dollars in global trade are lost because of non-tariff barriers to trade, which the WTO reported in 2012 were nearly twice as restrictive to trade as tariffs.[31] As an example, governments may set local content requirements that force firms to include a certain percentage of local components in their manufactured goods as a condition of market access. The Peterson Institute for International Economics estimated that such requirements alone reduced global trade by US$93 billion in 2013.[32]

The proliferation of nation-specific technical standards in the Canyon scenario presents another barrier to global trade in ICT products and services. National technical standards for reliability, compatibility, and security act as barriers because they are not keyed to international standards; thus they "create a wedge between domestic and foreign prices" and "affect trade flows."[33]

In 2013, such standards were already the most prevalent barriers to trade and were "reported to be the most difficult to comply with."[34] This continues in the Canyon scenario, where mutual recognition of certification schemes has slipped further away. Such disparate standards have many negative effects, including:

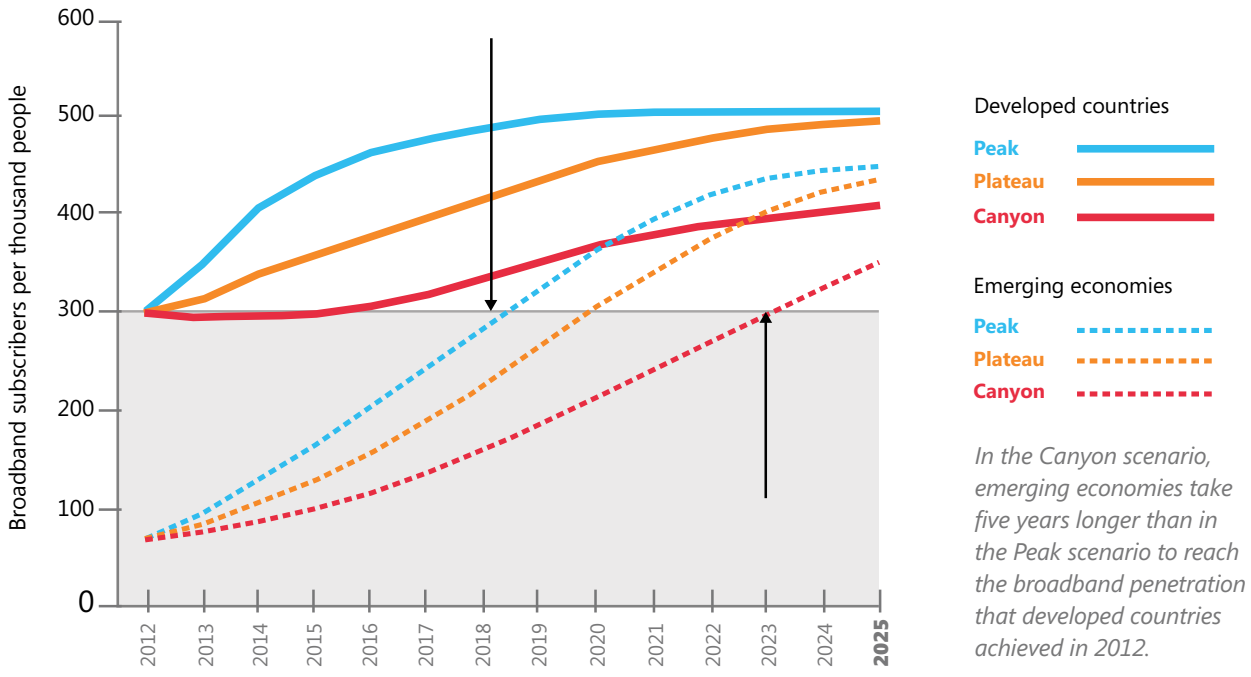
- Nation-specific standards that hamper the ability of technology companies to scale production, support, and infrastructure, dramatically raising costs and prices.
- Duplicative and onerous national standards and certification schemes that increase time to market, which is especially problematic in the time-sensitive technology industry.

International divisions fragment markets

Closed policies that limit global market access are the norm in the Canyon scenario, creating an international community that is divided at best and hostile at worst. These divisions occur at both economic and political levels. The collaboration and knowledge transfer that fuels technological development and widespread ICT adoption occurs only in small groups of countries or opportunistic bilateral arrangements.

An important consideration is how to maximize engagement in global value chains, which the Organization for Economic Cooperation and Development (OECD) defines as "all the activities that firms engage in, at home or abroad, to bring a product to the market, from conception to final use." The OECD found that countries that did not participate in open cross-border flows of digital information experienced a drop of over 60 percent in global ICT value chains between 1995 and 2009.[35] When countries are excluded from these opportunities, or opt out from them, the losses can be more than just financial.

Figure 9. ***Cyber 2025 Model Projections: Broadband Subscribers per Capita, 2012–2025***



In the Canyon scenario, emerging economies take five years longer than in the Peak scenario to reach the broadband penetration that developed countries achieved in 2012.

Just as hostile business environments, protectionist trade policies, and nation-specific standards in the Canyon scenario "disrupt the global market by fragmenting it,"[36] they also lead to the fragmentation (intentional or otherwise) of the Internet. This outcome is made more likely by the increasing frequency and severity of cyberattacks, which cause governments to respond with more restrictions that result in further fragmentations.

Business and economic factors restrict ICT development

Economic development falls short

Canyon countries see slower ICT development, uneven ICT access, fragmented ICT systems, and high cybersecurity risks. These problems worsen the poor economic conditions that the Cyber 2025 Model forecasts for Canyon. Where strong growth does occur, it is uneven and limited to specific countries or to specific industries within them.

Canyon countries, industries, and consumers that benefit from some economic growth and ICT use are limited. Domestic industries favored by governments due to political ties, state ownership, or connection to the military have great advantages compared to industries without such support. According to the Cyber 2025 Model, mobile computing still grows in the Canyon scenario, but consumers and businesses are forced to choose between fragmented proprietary systems that are secure but expensive, open systems used only for basic communication, or underground systems that are used by cyberactivists and criminals.

Limited research and development investments stifle opportunities

The unfavorable economic conditions and business environment in Canyon countries result in low investment levels, especially in research and development, and this seriously hinders the transformative potential of ICT.

In emerging economies, investment from foreign sources is especially important. A study conducted at the University of Redlands emphasizes that in these countries, technology use, expenditure, and infrastructure are most affected by foreign direct investment and governments setting ICT as a priority.[37] In the Canyon scenario, the technological progress and adoption in emerging economies is thus seriously limited by low foreign investment and by misguided or restrictive government approaches.

Restrained R&D and low foreign investment create an environment that does not support innovation in the Canyon scenario, and government policies aggravate the situation. The Information Technology and Innovation Foundation (ITIF) identifies two key ways in which national policies in particular thwart innovation.

First, innovative industries need access to large, global markets to cover their high fixed costs of R&D and design.[38] The significant trade barriers in the Canyon scenario inhibit the economic growth of innovative industries by limiting the abilities of these industries to scale their businesses. Profits are lower because of higher production and market-access costs for foreign firms and because of higher prices on imported goods. Altogether, this makes ICT products and services either unprofitable or very expensive, and it also leaves fewer resources for reinvestment in innovation.

Second, weak protection of intellectual property (IP) and forced technology transfers mean companies are less able to recover the costs of the initial research and development required to develop the IP. The companies receive less than market price, with fewer profits available for reinvestment in innovation.[39]

Investments in R&D not only help develop new technologies, but aid in their adoption. The Cyber 2025 Model indicates that investments in R&D are the second most important factor contributing to the growth of mobile Internet subscriptions, after mobile phone ownership.

In the Canyon scenario, business productivity and efficiency gains continue, but they do not significantly advance economic or socioeconomic development. Once again, emerging economies are the greatest losers of productivity improvements.

Social conditions limit the potential of ICT

Demographic changes overwhelm unprepared countries

Unprepared for demographic shifts, Canyon countries struggle to adequately serve either aging populations who strain economic growth or youthful populations who cannot find employment and create social unrest.

The Cyber 2025 Model points to mounting public debt as a key characteristic of the Canyon scenario, with the most important driver being the increasing number of people over age 65.[40] Burdened by debt, developed countries are forced to introduce austerity measures that could curtail short-term growth and raise political tensions.[41] In the long term, this debt limits the ability of Canyon governments to invest in education, private sector development, and technological growth.

Emerging economies with large populations of youth fall short of fulfilling the economic potential that could have been possible with better workforce alignment.

Workforces are unable to meet market needs

National workforces in the Canyon scenario lack the skills required to meet market needs and support ICT development. This, coupled with protectionist policies, limits talent mobility, increasing the skills gap.

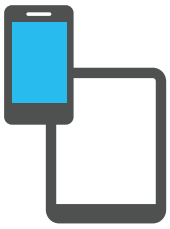
The interrelated socioeconomic conditions of Canyon directly hinder the access of many people to the potential benefits of ICT. For example, education systems are not able to fully use ICT to propel improvements or expand opportunities beyond national borders. Given the importance of ICT in bolstering education and the role education plays in promoting ICT adoption, the limited growth of each contributes to the resulting decline of the other.

Beyond insufficient formal education systems, Canyon countries also fall short of adequately preparing graduates for employment after school. Young people in the Canyon scenario face similar problems, despite the extreme need for employees in many countries.

Continual skills training helps workers remain marketable to employers and increases workforce productivity. In Canyon, governments and businesses fail to focus on lifelong skills development, despite the possibility of using ICT to implement low-cost solutions.

Cybersecurity characteristics of the Canyon scenario

TECHNOLOGY FOUNDATIONS



- Lagging broadband deployment in emerging economies will limit a range of ICT opportunities, including hindering foreign direct investment and local innovation. Despite growth in mobile subscriptions, the lack of modern infrastructure will constrain the government and its citizens in exploiting the benefits of cloud computing and the Internet of Things.
- In developed countries, governments seek to control technology both through domestic regulation and by limiting the use of global ICT products. As a result, ICT providers are unable to adequately address a country's cybersecurity needs, leaving the population with outdated and vulnerable technology.

THREAT ENVIRONMENT

- Cyberattacks ranging from simple crime to the intentional acts of nation-states plague governments and their citizens. As technology development has slowed, these relatively fragile infrastructures are often more vulnerable to attack. A lack of trained individuals to respond to attacks has limited the ability of countries to respond effectively. Continued attacks have distracted from more fruitful economic and societal activities.
- Hackers and cybercriminals in emerging economies overwhelmingly focus their attention on Internet users in the developed world. Governments, particularly in developed countries, may invest in offensive cybertechnologies for espionage instead of investing in cybersecurity technologies to support economic growth.

GLOBAL COOPERATION

- Countries will foster an environment of mistrust and animosity toward the global community, adopting cybersecurity policies that discourage collaboration. This will be exacerbated by a world where state-sponsored cybertheft and cyberattacks are more the norm than the exception.
- With increasing levels of malfeasance in cyberspace, some countries will feel besieged and will enact restrictive cybersecurity policies in response to each crisis that arises, leading to confusion and incompatibility.

Countries will foster an environment of mistrust and animosity toward the global community, adopting cybersecurity policies that discourage collaboration.

With increasing levels of malfeasance in cyberspace, some countries will feel besieged and will enact restrictive cybersecurity policies in response to each crisis that arises, leading to confusion and incompatibility.

EDUCATION	
	• Education, and particularly STEM education, is likely to be one of the earliest casualties in the shrinking budgets of emerging economies, leading to an overall decline in ICT growth as the largest potential talent pool will not be filling desperately needed high-tech jobs. • The limited job opportunities for those individuals trained for ICT will lead some to consider careers in cybercrime as an alternative.
TALENT MOBILITY	
	• Developed countries experience a critical talent gap driven, in part, by their aging populations, increasing costs of education, limited pool of STEM graduates, and inflexible immigration policies. They wall themselves off from global ICT talent, which constrains their ability to innovate. • Emerging economies may not be able to offer economic opportunity for their increasingly skilled workforces. Poor regulatory quality and lack of market access could spark a talent exodus and further erode national opportunities for innovation. Over the long term, technical talent from emerging economies will migrate to other markets that will provide opportunity and growth.
TRADE	
	• Market access is severely limited as mutual suspicions about the cybersecurity intentions of nations overcome trust in the global trading system. • Global trade negotiations halt as national security priorities displace interests in liberalized trade, thereby limiting global cooperation towards the flow of the data and devices that power ICT growth and development.

Conclusion and Recommendations

Cyberspace 2025 will not be a homogenous world of one terrain—Peak, Plateau, or Canyon. Like physical terrain, cyberspace will be a topographical mix. The question is what will the proportions be and how will the mix of high-performing, stalled, or declining countries impact the broader landscape in cyberspace.

This report highlights the transformative power of technology and connectivity, demographic shifts in developed and emerging economies, and the growing gaps in skills that support a highly Internet-dependent world. The future opportunities and risks are closely tied to policy decisions—today's policy decisions.

Conclusion

Change is happening. The terrain of cyberspace in 2025 is being shaped by the decisions that are currently being debated and made in capitals around the world. The countries that recognize it can help their citizens and economies (whether developed or emerging) thrive in the next decade and beyond.

This paper has presented three views of the world and cyberspace in 2025: Plateau, Peak, and Canyon. Most will naturally want the Peak scenario to come to fruition, but the myriad policy decisions that ultimately enable such a scenario are complex. Policymakers often must make decisions in isolation and may not consider the impact on innovation or security. Yet in a highly connected world, policy matters are in reality more and more connected. Success from this point forward is about grounding today's decisions in the desired future.

Navigating the future terrain of cyberspace requires a sound understanding of the trends across people, data, and devices and the relationships among them. By the year 2025, there will be a device-rich global north and a people-rich global south. No matter the hemisphere, the vast majority of new Internet connections will be mobile. In this hyperconnected world, the security and stability of the Internet will take on even greater importance to governments, businesses, and citizens.

While connectivity to and dependency on the Internet are expanding, the availability of expertise to build, support, and secure it is contracting. By the year 2025, over four billion people and countless devices will be connected to the Internet, and there will be nearly 20 million STEM graduates annually, with more than three quarters hailing from emerging economies. This puts stress on existing risk-management capabilities across all three scenarios for both developed and emerging economies.

Cybersecurity is one of the most challenging aspects of risk management. The Cyber 2025 Model provides a compass for evaluating directional changes in literacy, education, immigration, debt, and connectivity over time. The three scenarios presented in this paper provide a framework to evaluate the cybersecurity implications of the world in 2025.

There is no one-size-fits-all answer for attaining the Peak scenario. However, these foundations can help guide policymakers as they shape the specific terrain for their countries and begin to build the regional and global landscape of cyberspace in 2025.

Recommendations

Commit to an open, free Internet where privacy is protected. Governments should promote widespread adoption of online services by providing incentives, fostering user confidence, and developing consistent and clear guidelines for online service providers, including in the areas of privacy and security.

Governments can help foster free expression and access to information by showing restraint in imposing restrictions on Internet content and online anonymity, and by engaging in intergovernmental dialogue and cooperation. Governments can also develop a legal framework that includes innovation-friendly, nondiscriminatory, and predictable rules that govern online services vendors and offer clear guidelines for handling personal data.

Countries with ready access to an educated and skilled workforce are better positioned for sustained economic progress and job growth. Building an appropriately trained local talent pool requires strong science, technology, engineering, and mathematics (STEM) skills.

Advance cybersecurity risk management and coordination. The future will bring many changes in technology, and enable new scenarios for the use of technology. As technology evolves, so too will the sophistication of threats. Policymakers should place a strong emphasis on advancing the discipline of risk management to match the evolving threat landscape of cyberspace. The expanding technology base and shrinking technical expertise make investment in cybersecurity risk management an imperative.

Investing in information-sharing and incident-response capabilities that are effective within a country and internationally will be essential to in supporting security, privacy, and reliability across the myriad devices and scenarios that will shape the future of cyberspace. Collaboration across the public and private sectors nationally and internationally will be a defining theme for achieving a Peak scenario, and policymakers should ensure that policy frameworks and legislation support it.

Harmonize laws and standards affecting cybersecurity. Given the nature of the Internet, developing global ICT laws and standards rather than ones that are unique to each nation is an important principle. Harmonization of ICT law and international standards promotes understanding and predictability, enables collaboration on problem solving among countries, and helps to establish a more secure Internet. ICT development follows suit, in that creating products and services to meet hundreds of differing national requirements is unworkable, and will slow their development and hinder innovation, domestically and internationally.

Promote global free trade. Global growth and prosperity rely on a shared commitment by governments to combat protectionism and keep markets open. Governments can expand technology access for businesses by building upon existing trade agreements and forging new ones that eliminate barriers to trade. Such trade agreements can also expand investment opportunities, preserve consumer choice, and promote the dissemination and adoption of new technologies. Because businesses depend on the ability to store, transfer, and process data over global networks, trade agreements should guarantee the free flow of data across borders and prohibit local storage requirements.[42]

Invest strategically in infrastructure and research and development. More than 2.5 billion people worldwide have Internet access[43]; the number of users with broadband connections is a modest fraction of this number. Broadband access remains unaffordable for most of the world's people, but strategic investment by governments, advances in technology, and flexible regulation can dramatically reduce the cost of that access.

Improving global baselines for ICT capabilities in emerging economies, including software development, operations, response, policy, and risk management, is also vital. One key United Nations forum of international experts in its 2013 report [44] stated:

> "Capacity-building is of vital importance to an effective cooperative global effort on securing ICTs and their use. Some States may require assistance in their efforts to: improve the security of critical ICT infrastructure; develop technical skill and appropriate legislation, strategies and regulatory frameworks to fulfill their responsibilities; and bridge the divide in the security of ICTs and their use."

Government-funded research at universities and labs stimulates innovation and helps to train the next generation of scientists and engineers.

Enable talent mobility and retention. Countries with ready access to an educated and skilled workforce are better positioned for sustained economic progress and job growth. Building an appropriately trained local talent pool requires strong science, technology, engineering, and math (STEM) skills. Where talent shortages exist, governments can bridge the gap by attracting expertise from other countries. Regulatory frameworks should provide appropriate flexibility so employers can expand their operations and develop their workforce while maintaining worker protections within a range of workforce models. Governments that work to remove legal, regulatory, and practical barriers to importing and retaining talent can best take advantage of opportunities for economic growth.

Support the education of a modern workforce. If governments are to maintain and strengthen their ability to compete globally, they must adapt and improve their education systems to prepare students for the global economy by raising educational and teaching standards, rewarding effective educators, and providing teachers with the technology, support, and tools they need. Governments should also promote interest and training in STEM skills, which are needed for a broad array of readily available and high-paying jobs. For example, computer science is the foundation of today's innovation economy, but too few students have access to computer science instruction.

Develop cybersecurity norms for stability and security in cyberspace. Policymakers should analyze and prioritize existing cybersecurity best practices at national, regional, and international levels and determine where global principles or standards need to be developed. Key areas to explore should include confidence-building measures, responses to security incidents, assessment and mitigation of risk to critical ICT infrastructure, management of cyberrisk, supply chain security, protecting core encryption, and trust mechanisms of the Internet. In addition, policymakers should develop a set of cooperative measures for trust, stability, and reliability in cyberspace, with appropriate levels of responsibility for the public and private sectors, including at the international level.

Additional cybersecurity resources

Cybersecurity: Cornerstone of a Safe, Connected Society
aka.ms/cybersecurity-cornerstone

Developing a National Strategy for Cybersecurity
aka.ms/national-strategy

Five Principles for Shaping Cybersecurity Norms
aka.ms/cybersecurity-norms

Critical Infrastructure Protection
aka.ms/CIP-Concepts

Summary of scenario forecasts

The table below summarizes select forecast elements from the Cyber 2025 Model for key metrics in the areas of technology, economy, government, and education and their change from 2012.

		ECONOMIES	PEAK	PLATEAU	CANYON
TECHNOLOGY	Broadband Internet subscriptions per capita	Developed	.496 67% CHANGE	.491 65% CHANGE	.412 39% CHANGE
		Emerging	.441 538% CHANGE	.431 65% CHANGE	.344 397% CHANGE
	Mobile Internet subscriptions per capita	Developed	1.126 60% CHANGE	1.024 45% CHANGE	.960 36% CHANGE
		Emerging	.766 403% CHANGE	.531 249% CHANGE	.499 227% CHANGE
ECONOMY	Annual disposable income	Developed	US$5.8B 26% CHANGE	US$34.6B 19% CHANGE	US$32.6B 12% CHANGE
		Emerging	US$5.8B 81% CHANGE	US$5.5B 73% CHANGE	US$5.3B 65% CHANGE
	Expenditure on R&D per capita	Developed	US$1,429 30% CHANGE	US$1,329 20% CHANGE	US$1,231 12% CHANGE
		Emerging	US$114 103% CHANGE	US$108 92% CHANGE	US$101 81% CHANGE
GOVERNMENT	Public debt as a percentage of GDP	Developed	112% 2% CHANGE	130% 19% CHANGE	136% 24% CHANGE
		Emerging	36% 7% CHANGE	40% 15% CHANGE	43% 25% CHANGE
	Regulatory Quality Index score	Developed	1.41 8% CHANGE	1.36 3% CHANGE	1.30 -1% CHANGE
		Emerging	-0.12 53% CHANGE	-0.16 33% CHANGE	-0.21 13% CHANGE
EDUCATION	STEM graduates per 1,000 people	Developed	3.12 63% CHANGE	3.05 59% CHANGE	2.98 56% CHANGE
		Emerging	3.02 87% CHANGE	2.88 79% CHANGE	2.78 73% CHANGE

Appendix: Econometric Methodology

The key macroeconomic, socio-demographic, and technology indicators were modeled using two different regression-type approaches: linear panel data and non-linear S curve. Each model was developed for 80 countries using annual data between 1990 and 2012. The data was sourced from the Euromonitor International Passport database and its "Countries and Consumers" dataset.

The research covered several countries where data time series were limited or missing. To produce broad and encompassing models, the team entered imputed missing observations for the output indicators. This involved creating auxiliary first-difference panel data models on available data in other countries and predicting missing country data with available predictors (input indicators) such as GDP per capita and unemployment rate. Missing observations for predictor indicators were filled in with inflation-adjusted time series average values.

Modeling

Modeling approach selection

In order to select appropriate models for the analysis, the team investigated the nature of each output indicator and its relationship with the other output indicators. Stationary-output indicators (such as the Networked Readiness Index) were modeled using within-panel data models. For non-stationary output indicators (trending and highly cyclical indicators like disposable income), the first difference panel data models were estimated. When an output indicator portrayed a new product adoption process (like mobile Internet subscription rates), an appropriate non-linear S-curve approach was used. Individual models were joined in a system where some output indicators were used to predict other output indicators.

Preliminary modeling process

The team has tested more than one hundred different potential predictors and thousands of predictor combinations for each model. Due to a large number of potential predictors, the team used a separate predictor reduction process for each output indicator. More specifically, a bottom-up approach was carried out in which several alternative stable core models were augmented with additional explanatory variables through fully automated algorithms. To ensure that the models had sound statistical properties and robust economic motivation, the team continued to polish the results as discussed below.

Final model selection criteria and testing

Most importantly, every predictor had to be statistically important and economically relevant in order to be included in any given model. To investigate if indicators were statistically significant (in other words, that their effects on output indicators were significantly different from zero) T-tests or the equivalent were used. Each indicator also needed to have an appropriate directional effect (e.g., the effect of GDP on average disposable income should be positive) and be economically meaningful (e.g., microwave possession should not be the strongest predictor of Total GDP). Each predictor was carefully examined by the modeling team until a consensus was reached.

In addition all predictors included in a model needed to work well as a group. R-squared, F-tests, fit MAPE (mean average percentage error of a fit), and equivalent tests were used to determine the overall explanatory power of the model. Sometimes, replacing one significant indicator with a similar one produced a model with superior overall explanatory power.

Finally the model's capability to predict the future is tested with the help of out-of-time validation. Such validation works by trying to replicate the future situation in the present. A model is recalibrated on all years except the last one. Then the forecasts for the omitted year are generated using the model's forecasting algorithm. The forecasted values are compared with actuals by computing MAPE statistics. MAPE statistics are compared across alternative models. If a particular model's MAPE is suspiciously high, other model alternatives are investigated.

Forecasts

Baseline forecasts

The forecasts for each output indicator were generated by an algorithm based on econometric model results. The baseline forecasts for all predictor indicators (inputs to the algorithm) came from Euromonitor official forecasts, consensus forecasts by other third-party sources such as the OECD and World Bank, and in-house expertise.

Optimistic and pessimistic forecasts

Optimistic and pessimistic scenarios of all predictors (input indicators) were generated by analyzing how much countries fluctuated from their long-term trends in individual years over the 1990–2012 period. For example, to create the optimistic forecast for GDP in Germany, the relative deviations from average historical growth rates for all Western European countries during all available years would be collected, ranked from smallest to largest, and grouped by deviation size. These groupings would then be used to select an economically meaningful deviation percentile for GDP in the region, such as top 15 percent for the optimistic forecast and bottom 10 percent for the pessimistic forecast. In this example, if (a) the top 15 percent were to be 2.5 percentage points above the trend, and (b) the baseline forecast were to predict GDP growth in Germany at 2.3 percent, then (c) optimistic GDP growth in Germany in the next year would be 2.3+2.5=4.8 percent.

After similar analysis was done for all predictors, pessimistic and optimistic scenarios for each of the 10 outputs were computed.

Growth decomposition

Once the forecasts were finalized, each predictor's contribution to the growth of a given output indicator was calculated. This process is called growth decomposition. For example, annual disposable income growth of 15 percent over the 2012–2025 period could be decomposed, revealing that 10 percent of the 15 percent is driven by total GDP growth, negative 1 percent by unemployment rate, and 6 percent by the remaining factors.

Growth decomposition gives more practical information than model coefficient estimates because it combines the direction of a given predictor's effect with the likely change in the predictor over the period in question. Piecing the growth pattern together from all predictors helps to identify the most important drivers of growth.

Contributors

EUROMONITOR

Arunas Daujotis

Yuji Fukunaga

Mike Jozwik

Stephanie Landers

Corey Palmer-Rehorst

Jennifer Paruch

Tomas Rinkunas

Laju Tripathi

MICROSOFT

Erin English

Alison Massagli

Endnotes

1 See the World Economic Forum's annual *Global Risks* reports, starting with the first edition in 2006, www.weforum.org/issues/global-risks.

2 For a detailed description of this process, see the Appendix.

3 David Burt, Paul Nicholas, Kevin Sullivan, and Travis Scoles, *The Cybersecurity Risk Paradox* (Microsoft, January 2014), PDF, aka.ms/risk-paradox.

4 Michael DeGusta, "Are Smart Phones Spreading Faster than Any Technology in Human History?" *MIT Technology Review*, May 9, 2012, aka.ms/Technology-Review-Smartphone.

5 *Mobile Cocooning: How Growing Reliance on Smart Devices Is Influencing Consumer Behaviour*, Euromonitor International, Sep 2013, aka.ms/Euromonitor_Mobile_Report

6 James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, *Disruptive Technologies: Advances That Will Transform Life, Business, and the* Global *Economy* (McKinsey Global Institute, May 2013), www.mckinsey.com/insights/business_technology/disruptive_technologies.

7 Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything* (Cisco, April 2011), 3, PDF, www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

8 Richard Jackson, Neil Howe, and Keisuke Nakashima, *Global Aging and the Future of Emerging Markets* (Washington, DC: Center for Strategic and International Studies and Everest Capital Studies, 2011), 1, PDF, https://csis.org/files/publication/110307_Global_Aging_Future_of_Emerging_Markets.pdf.

9 The Cyber 2025 Model

10 Mauricio Soto, Baoping Shang, and David Coady, "New Projections of Public Health Spending, 2010-50" in *The Economics of Public Health Care Reform in Advanced and Emerging Economies*, ed. Benedict Clements, David Coady, and Sanjeev Gupta (Washington, DC: International Monetary Fund, 2012), 37-54, aka.ms/IMF-Health-2012.

11 Jackson, Howe, and Nakashima, *Global Aging*.

12 World Economic Forum, *Stimulating Economies through Fostering Talent Mobility* (Geneva: World Economic Forum, 2010), 7, PDF, www3.weforum.org/docs/WEF_PS_TalentMobility_report_2010.pdf.

13 Richard Dobbs, Anu Madgavkar, Dominic Barton, Eric Labaye, James Manyika, Charles Roxburgh, Susan Lund, and Siddarth Madhav, executive summary of *The World at Work: Jobs, Pay, and Skills for 3.5 Billion People* (McKinsey Global Institute, June 2012), PDF, aka.ms/MGI-Global-Labor-2012.

14 "Higher Education in Science and Engineering," in *Science and Engineering 2012* (Arlington, VA: NSF National Center for Science and Engineering Statistics, 2012), www.nsf.gov/statistics/seind12/c2/c2h.htm.

15 For more details on the theory of "innovation mercantilism," see Michelle A. Wein and Stephen J. Ezell, *The 10 Worst Innovation Mercantilist Policies of 2013* (Washingon, DC: Information Technology and Innovation Foundation, 2014), PDF, www.itif.org/publications/10-worst-innovation-mercantilist-policies-2013.

16 World Economic Forum, *2002 Annual Report of the Global Digital Divide Initiative* (Geneva: World Economic Forum, 2002), PDF, www.weforum.org/pdf/Initiatives/Digital_Divide_Report_2001_2002.pdf.

17 Gianluca Misuraca, David Broster, and Clara Centeno, "Digital Europe 2030: Designing Scenarios for ICT in Future Governance and Policy Making," supplement, *Government Information Quarterly* 29, no. S1 (2012): S121-S131, dx.doi.org/10.1016/j.giq.2011.08.006.

18 Catherine Saez, "15 Years Later, Prospects For WTO Information Technology Agreement Examined," *International Property Watch*, May 15, 2012, aka.ms/Saez-ip-watch.

19 International Centre for Trade and Sustainable Development, "ITA Expansion Efforts Aim for Final Product List by July," *Bridges Weekly Trade News Digest* 17, no. 20 (2013): 10-11, ictsdorg/downloads/bridgesweekly/bridgesweekly17-20.pdf.

20 Allan Friedman, *Cybersecurity and Trade: National Policies, Global and Local Consequences* (Washington, DC: The Brookings Institution, 2013), 14, PDF, www.brookings.edu/research/papers/2013/09/19-cybersecurity-trade-national-policies-global-local-friedman.

21 "CSA Security, Trust & Assurance Registry (STAR)," Cloud Security Alliance, cloudsecurityalliance.org/star

22 Dirk Swart, *Africa's Technology Futures: Three Scenarios*, the Pardee Papers, no. 14 (Boston: Frederick S. Pardee Center for the Study of the Longer-Range Future at Boston University, 2011), 5, PDF, aka.ms/Swart-Africa-Tech.

23 Organization for Economic Cooperation and Development (OECD), "Generating Value from Health ICTs," in *Improving Health Sector Efficiency: the Role of Information and Communication Technologies*, OECD Health Policy Studies (Paris: OECD Publishing, 2010), 32, PDF, ec.europa.eu/health/eu_world/docs/oecd_ict_en.pdf.

24 Microsoft Research Connections Team, "Workshop highlights medical uses of Kinect technology," *Microsoft Research Connections Blog*, January 10, 2014, aka.ms/Microsoft-Research-Connections.

25 Center for Technology and Aging, *Technologies to Help Older Adults Maintain Independence: Advancing Technology Adoption* (Oakland: Center for Technology and Aging, 2009), PDF, www.techandaging.org/briefingpaper.pdf.

26 Organization for Economic Cooperation and Development, *Better Skills, Better Jobs, Better Lives: A Strategic Approach to Skills Policies* (Paris: OECD Publishing, 2012), 24, PDF, skills.oecd.org/documents/OECDSkillsStrategyFINALENG.pdf.

27 William D. Eggers and Joshua Jaffe, *Gov on the Go: Boosting Public Sector Productivity by Going Mobile* (Deloitte University Press, February 18, 2013), 2, PDF, dupress.com/articles/gov-on-the-go.

28 Ibid.

29 A 2013 Organization for Economic Cooperation and Development working paper finds that "innovation-specific policies such as R&D tax incentives, direct government support and patent rights are found to be successful in encouraging the innovative activities associated with higher productivity growth," even though "direct empirical evidence of the positive effects of these policies on productivity is less forthcoming."
Ben Westmore, *R&D, Patenting and Growth: The Role of Public Policy* OECD Economics Department Working Papers, no. 1047 (Paris: OECD Publishing, 2013), 2, PDF, aka.ms/westmore-rd.

30 *Hearing: Digital Trade in the U.S. and Global Economies Before the United States International Trade Commission*, Investigation No. 332-531 (2013) (written testimony of Stephen J. Ezell, Senior Analyst, Information Technology and Innovation Foundation), 1, PDF, www.itif.org/publications/hearing-digital-trade-us-and-global-economies.

31 World Trade Organization (WTO), *World Trade Report* (Geneva: WTO Publications, 2012), PDF, www.wto.org/english/res_e/booksp_e/anrep_e/world_trade_report12_e.pdf.

32 Gary Clyde Hufbauer, Jeffrey J. Schott, Martin Vieiro, and Erika Wada, *Local Content Requirements: A Global Problem* (Washington, DC: The Peterson Institute for International Economics, September 2013), xxi, bookstore.piie.com/book-store/6802.html.

33 Olivier Cadot, Sebastian Saez, and Maryla Maliszewska, "Non-Tariff Measures: Impact, Regulation, and Trade Facilitation," in *Modernizing Border Management*, ed. Gerard McLinden (Washington, DC: The World Bank, 2010), quoted in Friedman, *Cybersecurity and Trade,* 13, works.bepress.com/ocadot/24.

34 Friedman, *Cybersecurity and Trade*, 13.

35 *Hearing: Digital Trade in the U.S. and Global Economies*.

36 Friedman, *Cybersecurity and Trade*, 13.

37 James B. Pick and Rasool Azari, "Worldwide digital divide: influences of education, workforce, economic, and policy factors on information technology" in *Proceedings of the 2007 ACM SIGMIS CPR conference on Computer personnel research: The global information technology workforce* (New York, NY: ACM, 2007), 78-86, doi:10.1145/1235000.1235019.

38 Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, executive summary of *Localization Barriers to Trade: Threat to the Global Innovation Economy* (Washington, DC: The Information Technology and Innovation Foundation, September 2013), 4, PDF, www2.itif.org/2013-localization-barriers-to-trade-exec-summary.pdf.

39 Ezell, Atkinson, and Wein, *Localization Barriers,* 5.

40 The Cyber 2025 Model

41 Dun and Bradstreet, *D&B's Global Economic Outlook to 2017* (Short Hills, NJ: Dun and Bradstreet, 2013), 4, PDF, www.dnb.com/content/dam/english/economic-and-industry-insight/global_economic_outlook_to_2017.pdf.

42 Microsoft, *2014 Global Public Policy Agenda: Real Impact for a Better Tomorrow*, (January 2014), 3, PDF, aka.ms/2014_Public_Policy_Agenda.

43 "Internet World Stats: Usage and Population Statistics," Miniwatts Marketing Group, last modified April 25, 2014, www.Internetworldstats.com/stats.htm (2012).

44 UN General Assembly, "Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", June 24, 2013, 10, PDF, aka.ms/GGE-Report.