Atlantic Council

THE FREDERICK S. PARDEE CENTER FOR INTERNATIONAL FUTURES
EXPLORE, UNDERSTAND, SHAPE

ZURICH

Risk Nexus

Overcome by cyber risks? Economic benefits and costs of alternate cyber futures

Contents

Foreword

Frederick Kempe,
President and CEO
Atlantic Council

Cecilia Reyes,
Chief Risk Officer
Zurich Insurance Group

The globalization of value chains, increased financial integration, rapid urbanization, and the Internet's ubiquity have all accelerated worldwide economic growth over the past few decades. Unfortunately, these same developments have also significantly increased our vulnerability to external shocks and global crises. With risks mounting and traditional systems of control weakening, now is the time to ask: do the risks of being connected outweigh the benefits to global economic growth?

Zurich Insurance Group and the Atlantic Council's Brent Scowcroft Center on International Security are engaged in a multi-year partnership to examine that question as a continuation of our previous collaboration on systemic cyber risks. Our groundbreaking report, *Beyond Data Breaches: Global Aggregations of Cyber Risk*, published in April 2014 was our first answer on this topic and went well beyond well-known common cyber risks to explore the potential for broader cyber shocks.

That first report examined how a 'Lehman Brothers moment' at a too-big-to-fail communications technology firm, wiping out droves of vital consumer data, might cause a cascading failure throughout the wider economy.

This second report in the series expands on that scenario, building on this concept of 'cyber sub-prime.' We use economic modeling tools to understand, for the first time, how cyber costs and benefits might affect global gross domestic product (GDP) over time and how we can steer ourselves towards the most rewarding futures.

The Atlantic Council's Brent Scowcroft Center on International Security teamed with the Pardee Center for International Futures at the University of Denver to conduct extensive quantitative analysis based on dozens of global sources and inputs – from Oxford University in the UK to Abu Dhabi, Sao Paulo, Montreal, Singapore, and Washington, DC.

After this open process, we modeled the economic benefits from information and communication technologies (ICT) and related cybersecurity costs. The difference between our model's best and worst forecasts through 2030 is a startling USD 120 trillion, or about 6 percent of cumulative global GDP, driven largely by accumulating costs from cyber incidents.

With this report, we hope to raise awareness about the need to work as a global community towards a more secure, resilient, and prosperous Internet for decades to come. Our specific recommendations for enhancing the cyber commons offer an initial roadmap for economists, technologists, cybersecurity practitioners and researchers, and perhaps the public as a whole.

The subsequent reports in this series, due in 2016, will use the model and methodology pioneered here to explore geopolitical and demographic risks.

Executive summary

> The accumulated global benefits of being connected should still outpace the costs through the year 2030 by nearly USD 160 trillion."

In 2030, will the Internet and related information and communications technologies (ICT) continue to drive global innovation and prosperity? Or, will that bright promise be swamped by an unstable and insecure Internet, so overwhelmed by non-stop attacks that it has become an increasing drag on economic growth? The answers, as far as we can predict, are not promising and mean the difference in tens of trillions of dollars in global economic growth over the next fifteen years.

So far, cyberspace has been safe enough, secure enough, and resilient enough for the past decades to re-invent nearly every industry, create a 'hyperconnected world,' and transform the global economy.

Unfortunately, these benefits come with an increased dependence on a shared, stunningly complex system-of-systems, which no one truly understands in its entirety. Most of the recent cybersecurity trends point to a darker future, with every year worse than the last: more data breaches, more disclosures of critical vulnerabilities, and more nations building and employing offensive cyber capabilities.

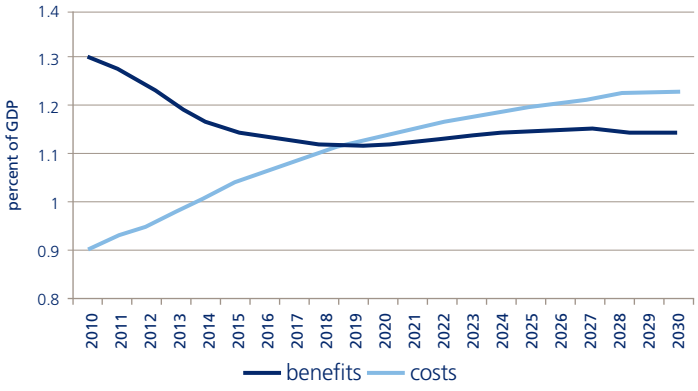
Teaming with the Pardee Center at the University of Denver, we modeled the economic benefits from ICT and the associated cybersecurity costs. To model the benefits, we researched the contribution to GDP of the ICT sector itself, the benefit of ICT to the rest of the economy, as well as the benefit to consumers. The costs included direct cybersecurity spending, the losses from cyber incidents, and opportunity costs because economies may not be making full use of ICT.

A future where the annual costs of being connected outweigh the benefits is not only possible, it is happening *now*. According to our project models, annual cybersecurity costs in high-income economies like the U.S. have already begun to outweigh the annual economic benefits arising from global connectivity.

For all economies, the inversion of costs and benefits is expected to occur within the next five years. In Latin America, it is expected before the year 2030, as the region bridges the digital divide. In the Asia-Pacific region, the inversion is expected sometime after that. (Figure 1)

This is the bad news.

Figure 1: ICT cyber benefits and costs, global annual totals, 2010-2030



Note: Using 5-year moving average

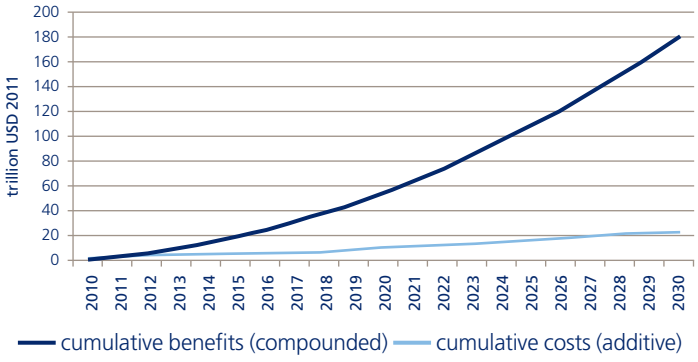
Source: IFs 7.15

Fortunately, there is good news, and it is actually pretty great.

Although the one-time costs of being connected are higher on an annual basis, benefits accumulate over time, as they tend to be made as long-term investments in productivity. In other words, cyber benefits tend to keep delivering each year after they are originally felt, whereas the costs tend to be experienced as 'one offs.'

In our Base Case, the accumulated global benefits of being connected should still outpace the costs through the year 2030 by nearly USD 160 trillion (constant 2011 US dollars), an 8 percent gain in the cumulative global GDP between 2010 and 2030.

Figure 2: ICT cyber benefits and costs, global cumulative totals, in USD trillion, 2010-2030



Source: IFs 7.15

Table 1: Expected GDP in 2030. This table adds context for interpreting the costs and benefits in the report, relative to the size of the global economy in 2030

Region	**Annual GDP in 2030** (at market exchange rate)	**Cumulative GDP** (at market exchange rate)
World	USD 135 trillion	USD 2,000 trillion
High-income economies*	USD 70 trillion	USD 1,200 trillion
U.S.	USD 24 trillion	USD 400 trillion

*World Bank definition

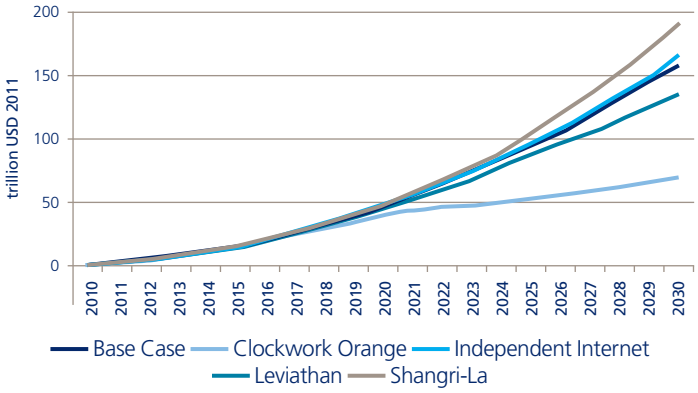
Cyber attackers dragging down the Internet might cost the world nearly USD 90 trillion."

We also examined four alternate futures. In the best future of *Cyber Shangri-La*, where technology booms are driven by strong cybersecurity, the recurring annual economic benefits result in a cumulative net global gain of USD 190 trillion by the year 2030 – about USD 30 trillion higher than that of the Base Case. In the worst future of a *Clockwork Orange Internet*, cyber attackers dragging down the Internet might cost the world nearly USD 90 trillion of potential net economic benefit[1]. In a *Leviathan Internet* future, governments impose strong Internet borders, and global benefits drop by around USD 20 trillion when compared to the Base Case and a fourth alternate future, the corporate-driven *Independent Internet*.

Steering towards these trillions of dollars of global economic benefits requires a range of actions today from states, companies, non-state groups, and individuals.

A strong and resilient Internet will be driven by a healthy non-state sector, supported when needed by governments. Avoiding the worst futures is a global collective action problem that requires a sense of joint stewardship over the Internet, needing actions that go far beyond just admonitions to 'improve cyber security.' We must also focus on improving resilience and, above all, international governance for the globe and the Internet.

Figure 3: ICT cyber net benefits or costs, global cumulative total, in USD trillion, by scenario, 2010-2030



About the Principal Investigators

Jason Healey is Senior Fellow for Cyber Statecraft at the Cyber Statecraft Initiative of the Atlantic Council's Brent Scowcroft Center on International Security and Senior Research Scholar at Columbia University's School of International and Public Affairs.

Barry Hughes is the John Evans Professor at the Josef Korbel School of International Studies at the University of Denver and Director of the Frederick S. Pardee Center for International Futures.

For more details on the model, data, and process used in this report, please see the companion report produced by the Pardee Center, available at **www.pardee.du.edu**

Premise explained

Newspaper headlines inundate us with stories about the risks associated with our increasingly interconnected lives and digitized economies: cyber failures and outages, espionage against (or indeed by) government agencies, massive data breaches involving tens of millions of retail and bank customers, and damaging and disruptive attacks by nations against one another.

Yet we still believe that the benefits of being connected are worth these risks. As individuals, we continue to buy new smartphones and apps and connect our houses, cars, and even medical devices to the Internet. At the same time, companies increasingly depend on connectivity to drive their business models, even outsourcing business-critical infrastructure through cloud computing and storage.

This report seeks to answer a critical risk management question for the twenty-first century:

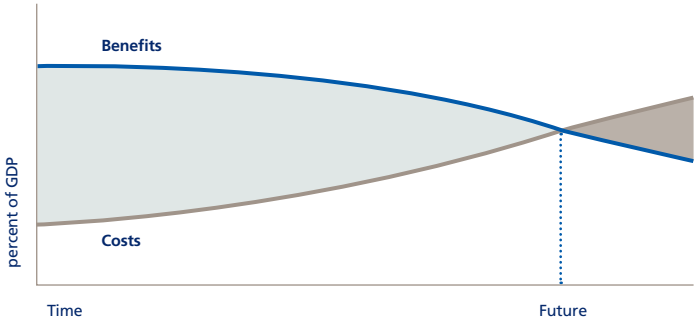
Will the risks of being interconnected start to outweigh the benefits?

Certainly, many cyber security experts have repeatedly warned us that a series of 'digital Pearl Harbors' or other catastrophes might tip the balance, causing security and response costs to outweigh the benefits from ICT to global GDP. Others, such as the techno-enthusiasts in Silicon Valley, imagine the question to be irrelevant, believing that they could always surf new waves of innovation and invention to stay ahead of the dangers. The truth probably lies somewhere in the middle. As the renowned cybersecurity expert Dan Geer has suggested, "[a] technology that can give you everything you want is a technology that can take away everything that you have."[2]

Economic modeling, even when based on limited data, is an important way to explore these kinds of alternate futures. At the beginning of the process of working on this report, the modeling team at the University of Denver's Pardee Center created two graphs to illustrate the above premise. Figure 4 shows that early on, the annual benefits of being interconnected far outweigh the costs but that theoretically, there could be an inversion at some point in the future.

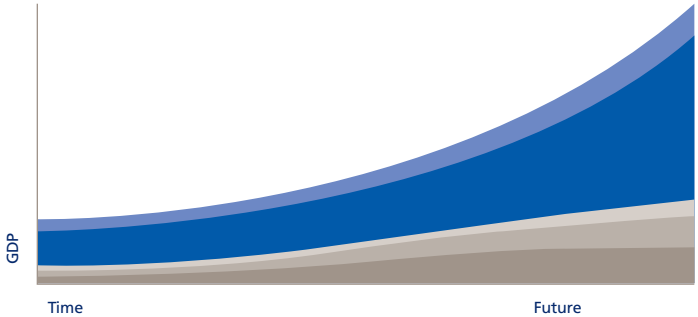
Cyber benefits keep delivering compounding rewards years after the initial investment, whilst the costs tend to be one-off expenses. So even after such a theoretical future inversion, the *accumulated* benefits might still continue to outpace costs, as shown in Figure 5. The project team then gathered data to feed the economic models to see if an inversion was likely to happen in the future and if the accumulated benefits would stay ahead of costs, Figure 5.

Figure 4: Illustration of a hypothetical future where costs outweigh benefits on an annual basis



Note: This graphic represents both costs and benefits as flows (percent of GDP)
Source: Authors' conception

Figure 5: Should annual costs (in stone) increase, the way benefits (in blue) compound over time suggests that the overall impact should still be positive



Note: This graphic illustrates the compounding benefits of ICT/cyber contributions to economic productivity and illustrates the growth of costs through simple annual additions
Source: Authors' conception

Box 1: An example of the balance of cyber benefits and risks: annual versus cumulative[3]

In 2013, Mom and Pop Dry Cleaners bought a computer to better manage their purchase of supplies. Their profits in 2009 had been USD 300,000, and the new computer helped them save USD 3,000 (1 percent) on supply costs in 2010 even after the initial capital investment.

Unfortunately, Pop downloaded malware, and the firm hired to clean their system charged USD 3,000 – a one-time cost that completely offset that year's savings. In 2014, they downloaded a software package to manage their customer database and used it, adding USD 3,000 to their profits.

Because the computer was still saving them money on supply ordering, Mom and Pop's total cyber benefit that year was USD 6,000. But they also paid USD 3,000 to another firm that greatly enhanced the security of their systems.

Then, in 2015, they downloaded more software allowing them to mail out specials and attract more clients, generating a surprisingly coincidental contribution to profit of USD 3,000. They again used their computer and earlier software purchases to recognize the savings in supply and benefits of the customer database for a total cyber contribution to profits of USD 9,000. Unfortunately, that same year, hackers broke through their new security system, and the firm that patched them up charged USD 4,500.

Evaluating the benefits of the path they started to follow in 2013, Mom said to Pop: "This year the annual risk-related costs of keeping these bloody systems more than offset the annual boost to profits (USD 3,000 minus USD 4,500). But the cumulative contributions to our profits keep compounding: USD 3,000 plus USD 6,000 plus USD 9,000 equals USD 18,000, while the risk-related costs we pay each year are one-time (USD 3,000 plus USD 3,000 plus USD 4,500 equals USD 10,500). Next year in 2016, I want to invest USD 3,000 to create a webpage and get the word out about our shop!"

The model and process

This report's quantitative findings are based on the International Futures (IFs) forecasting system, run by the University of Denver's Pardee Center for International Futures. The forecasting model was used as the primary tool to display and analyze historical data as well as to forecast and develop alternative future scenarios. The IFs model represents 186 countries in different stages of socio-economic development and adoption of ICT technologies. It encompasses a set of heavily integrated and rich models: demographic, economic, human development (education and health), physical (energy, agriculture, and infrastructure), and socio-political (governance and government finance).

The modeling team worked to produce a rough understanding of the relative benefits and costs of ICT. This is the first attempt to build exhaustive typologies of different cyber benefits and costs in order to compare them and provide an overall assessment of current benefits and costs.

The IFs forecasting model builds on this initial data using cross-country comparison and longitudinal series when possible. The model incorporates measures of ICT penetration or pervasiveness and of ICT spending as driving variables for future benefits and costs. It draws upon existing variables already in the IFs model, including GDP per capita and economic growth rates, to explore very different assumptions around the future of ICT and the implications of alternative possible scenarios.

The modeling started with a 'Base Case' estimate of how past trends might continue into the future, then examined four alternative scenarios that differ in critical ways.

However, this modeling was limited by the lack of comprehensive data, especially on the economic costs of adverse cybersecurity events. Roughly 150 different ICT-related data series were included in this analysis, and yet there was little comprehensive data across countries and time. For additional context, the Atlantic Council also organized a series of global meetings – from Oxford University in the UK to Abu Dhabi, Sao Paulo, Montreal, Singapore, and Washington, DC.

Due to the lack of comprehensive data and the fact that this was the first major attempt to model cyber benefits and costs, this report is correspondingly cautious on the findings. As Dan Geer, who specializes in metrics, has said, "it is the trend that matters... look at the shape" of the curves.[4] And the general trends identified in this report should help drive the global debate on cybersecurity problems and solutions.

For more details on the model, data, and process used in this report, please see and use the IFs model at http://www.pardee.du.edu, find the companion report produced by the Denver University's Pardee Center for International Futures at http://www.pardee.du.edu/cyber-benefits-and-risks-quantitatively-understanding-and-forecasting-balance, and use the dashboard for simplified computer or mobile device analysis of our forecasts at http://www.ifs.du.edu/ifs/frm_CyberDashboard.aspx

At least five of the top six game-changing technologies require strong cybersecurity to unlock the benefits and avoid significant, perhaps catastrophic costs."

Box 2: The promise and peril: new waves of technology

The benefits of technology are apparent everywhere, as is the ICT that has most obviously changed our lives:

- the personal computer, which took computers out of a dedicated room staffed only by technicians, and put them on desktops in our homes and offices;
- mobile technology, which took those connected computers off the desktop and put them into our pockets; and
- the Internet, which connects all those computers, no matter where they are on Earth.

But what are the next potentially game-changing technologies?

The McKinsey Global Institute (MGI) foresees twelve such technologies, many of which are heavily ICT dependent.[5] They are mobile Internet, automation of knowledge work, the Internet of Things (IoT), cloud technology, advanced robotics, autonomous and near-autonomous vehicles, next-generation genomics, energy storage, 3D printing, advanced materials, advanced oil and gas exploration and recovery, and renewable energy.

At least five of the top six (excluding perhaps the automation of knowledge work) require strong cybersecurity to unlock the benefits and avoid significant, perhaps catastrophic costs. Together, those top five security-dependent technologies could have potential economic impact by 2025 of between USD 13 trillion and USD 36 trillion, according to MGI.[6]

Though MGI puts IoT only in the third position, with potential economic upside impact of up to USD 6.2 trillion, according to the experts interviewed for this report, it probably has the highest potential security costs. The IoT connects the Internet to physical objects, from electrical generation and distribution down to automobiles, thermostats, baby monitors, and wearable fitness bands. This connectivity can unlock tremendous value and change lives and societies, but unfortunately security is rarely included.

These devices are typically far less secure than your computer or mobile phone, as there are few safety features – the software is probably infrequently checked for vulnerabilities, it is difficult to update with new software, and there is likely no security software to monitor for attacks.

As one report prepared for the President of the United States put it, "There is a small – and rapidly closing – window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations."[7]

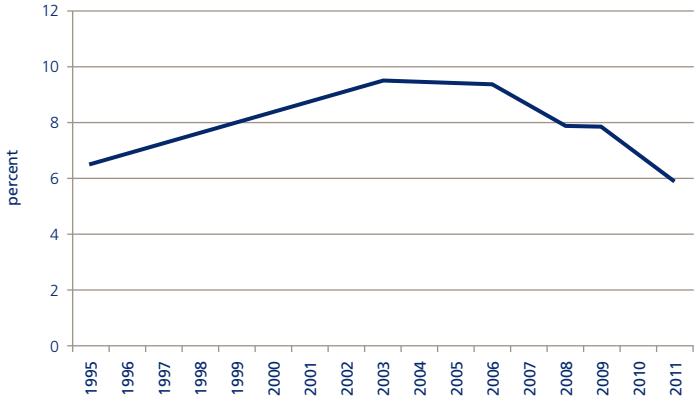
Unfortunately, that window has probably already closed.

Measuring the economic benefits of ICT

The benefits of ICT have emerged and have been changing the world from three main sources:

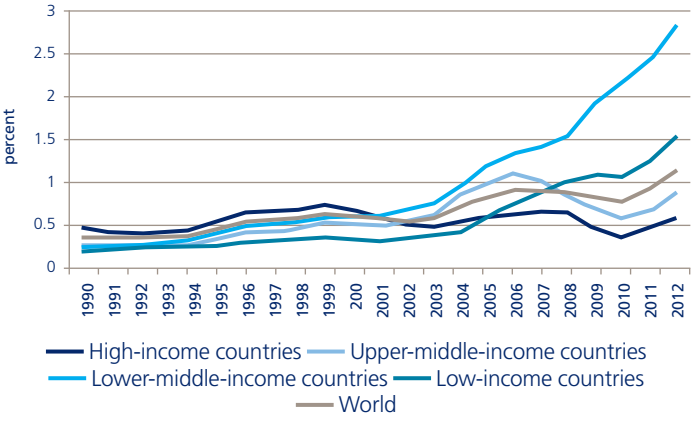
1. **Direct contributions from the ICT sector itself:** The direct value added to GDP by ICT sector companies (for example, from well-known major ICT companies like Apple, Microsoft, Intel, or Google) has been estimated to have grown to 9 percent of total business value added in Organization for Economic Co-operation and Development (OECD) countries; however, in large part due to the continuing decline in ICT costs, the direct value added has been falling over the past few years, bringing it back down to around 6 percent today (see Figure 6 for the information on OECD countries). The ICT sector share of GDP is still growing in developing countries but is relatively stable globally.
2. **ICT impact on productivity and GDP for the economy as a whole:** ICT doesn't just benefit the companies that make them, but the rest of the economy as well, including benefits to manufacturers, bankers, and retailers who use ICTs. These contributions are usually estimated to add between 20 to 30 percent to economic growth. This number translates to 0.6 to 1.5 percentage points of absolute contribution to global GDP growth (see Figure 7).
3. **Benefits to consumers:** The even harder-to-measure 'consumer surplus' refers to benefits consumers receive from ICT, from either rapidly decreasing prices or from improving capacity and quality at the same price (for example, from Moore's Law[8]). The same USD 1,000 buys a far more capable and productive computer now than it did ten years ago. The most convincing data we have found, however, suggest that consumer surplus contributions are about half of those from ICT's boost to the growth of the economy as a whole.

Figure 6: ICT value added as a percentage of total business sector value added, average of OECD countries



Source: OECD Factbook database, share of ICT value added, available at: http://www.oecd-ilibrary.org/economics/data/oecd-factbook-statistics/oecd-factbook_data-00590-en

Figure 7: ICT capital services' contribution to GDP growth, by World Bank country income group and world



Note: Simple cross-country averages of raw data used for each income grouping

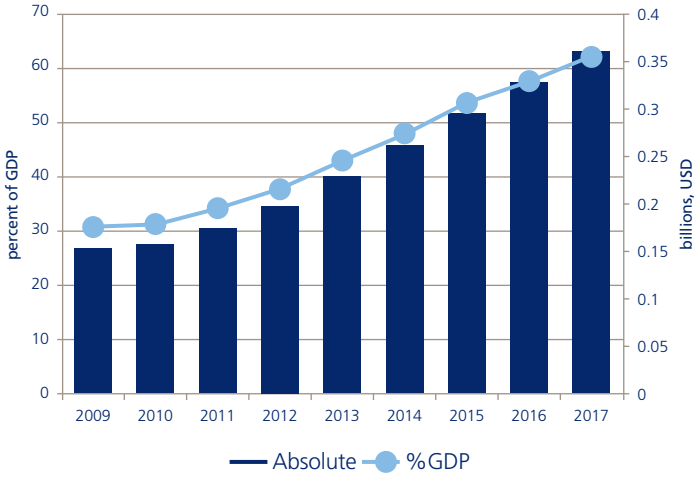
Source: The Conference Board Total Economy Database, contribution of ICT capital services to GDP Growth, 2014, available at: https://www.conference-board.org/data/economydatabase/index.cfm?id=27762

Measuring the economic costs of ICT

Data on the costs of an insecure Internet are very scarce and piecemeal, and not very confidence-inspiring. In general, there are three types of costs:

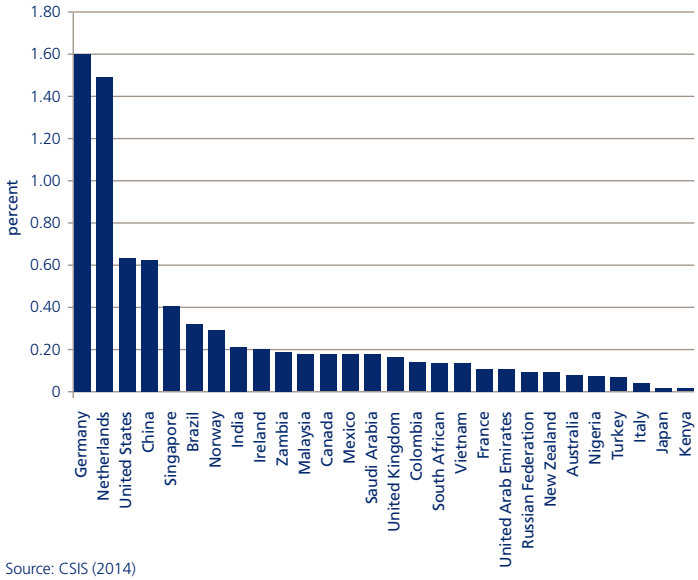
1. **Spending on cyber security:** The direct spending on cybersecurity solutions (such as firewalls and threat intelligence) is rising steadily, approaching 0.1 percent of global GDP and 0.35 percent of US GDP (see Figure 8).[9] Two forces may be driving these increases: the capabilities of attackers to carry out increasingly complex actions, and the growth in assets that are accessible via networks and therefore vulnerable to attacks.[10]
2. **Costs of adverse cyber events:** These include all the costs of a cyberattack or outage once it has occurred, from recovery costs to financial crime, the value of stolen intellectual property and related erosion of innovation, and the theft of confidential business information (like negotiating positions). According to 2014 estimates by the Center for Strategic and International Studies (CSIS), the costs of cybercrime range from 0.02 percent of GDP in Japan to 1.6 percent in Germany. Values for the U.S. and China are at 0.64 and 0.63 percent respectively, see Figure 9.[11]
3. **Opportunity costs:** These costs are the unrealized economic benefits of ICT, such as when companies forego using new technologies because of security concerns, or when nations chose not to embrace ICT for domestic policy reasons. For example, if ICT contributes to about one-fourth of global growth, North Korea, which has virtually no ICT sector, would be foregoing nearly all of that potential (and Cuba perhaps half due to its fledgling ICT sector).

Figure 8: Cybersecurity spending in the U.S., percent of GDP and USD billions, 2009-2017



Source: TIA's 2010-2017 ICT Market Review and Forecast, available at: http://test.tiaonline.org/resources/market-forecast

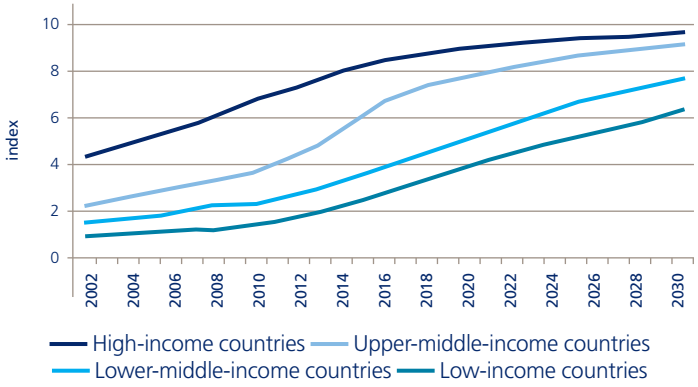
Figure 9: The cost of cybercrime and cyber espionage expressed as percent of GDP



Source: CSIS (2014)

Base case: Benefits and costs to 2030

Figure 10: ICT development index (ITU index replication), by World Bank country income group, 2002-2030



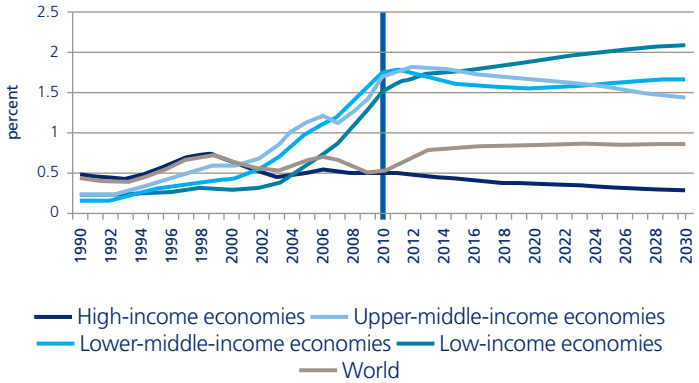
Source: Historical data (through 2013) from the ITU's ICT Development Index (ITU 2014). Forecast from IFs 7.15

The International Telecommunications Union (ITU) maintains an index of ICT development that helps us understand past patterns and forecast future ones.[13] Forecasts of mobile and broadband connectivity levels, which are major drivers of the index, suggest a convergence in the prevalence of ICT across economies of different income levels as connectivity becomes universal (see Figure 10). Of course, this is not the only possible outcome, as future waves of ICT (such as higher speeds, cloud computing, or IoT) might postpone saturation. Such alternate futures are discussed later in this report, while the Base Case forecast represents the ITU's rather conservative outlook.

The modeling of the costs and benefits of connectivity began with a 'Base Case.' The Base Case in the IFs integrated modeling system captures a continuation of past and current patterns. It paints a picture of where the world is headed if these general trends continue without interruptions from unforeseen, disruptive geopolitical, economic, or technological crises.[12]

Regarding **benefits**, the main driver of economic growth is ICT's contribution to other sectors. It may feel counterintuitive, given how much we can feel ICT changing the industries around us, but according to extensive economic research, this contribution has in fact been mostly flat or declining in high-income economies. Even so, ICT still provides about a 1 percent annual boost to GDP growth.

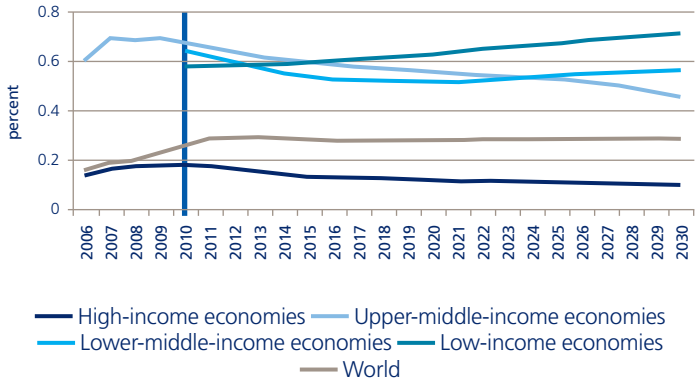
Figure 11: ICT cyber benefit, annual boost to GDP growth, by World Bank country income group, 1990-2030



Note: The graph uses a simple average of country values, because using a grouping of a few large GDP countries (e.g. China) can otherwise distort the data. The graph also uses a five-year moving average. The biggest discrepancy occurs between historical data and forecasts for lower-middle-income countries. In this area, our forecast may underestimate the future contribution of ICT, though the bubble of growth contributions in recent years may be temporary. Globally, there is strong continuity between historical data and forecasts.

Source: Historical data through 2012 are from Conference Board (2014a and 2014b). Data from 2010-2030 are from IFs 7.15

Figure 12: ICT cyber benefit, annual consumer surplus, by World Bank country income group, percent of GDP, 2006-2030



Note: Using 5-year moving average

Source: Historical data through 2010 are from OECD (2013). Data from 2010-2030 are from IFs 7.15

Since the overall size of the ICT sector has reached a roughly stable (or even declining) share of global GDP, the growth of that sector is unlikely to contribute much to growth rates of the average economy. The annual consumer surplus is much smaller, approaching 0.1 percent of GDP for high-income economies but up to 0.7 percent for low-income economies.

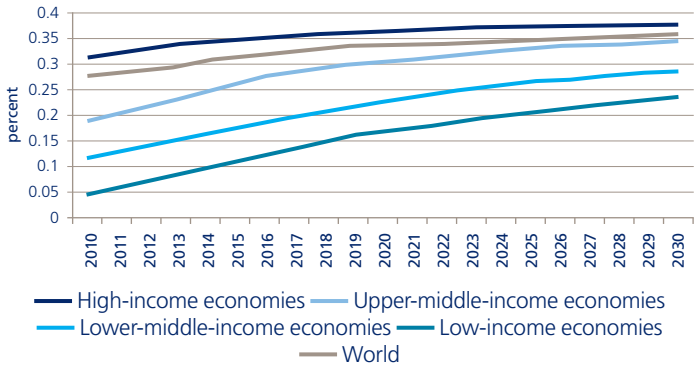
Direct global cyber security **costs** are forecast to continue to rise over the next fifteen years, though the spending curve does become flatter. In high-income economies, the direct spending on cybersecurity reaches nearly 0.4 percent of GDP by 2030 with low-income economies approaching 0.25 percent, as shown in Figure 13. In dollar terms, cybersecurity spending for 2015 is estimated at roughly USD 250 billion (in constant 2011 dollars), a cost that doubles by 2030 to nearly USD 500 billion.

By 2030, the cost of adverse events could reach USD 1.2 trillion, or perhaps 0.9 percent of global GDP (see Figure 14). Here, low-income economies are highly dependent on the Internet, but lack of security and resilience impose a relatively higher cost of about an additional 0.2 percent of GDP.

Opportunity costs from not taking advantage of ICT capabilities are comparatively very low, typically below 0.1 percent. At the beginning of this project, we expected such foregone benefits to be significant because of cybersecurity fears, but as Beau Woods, one cybersecurity expert interviewed for this report, explained it, "decisions are usually made with implicit trust that cyber security measures will work."[14]

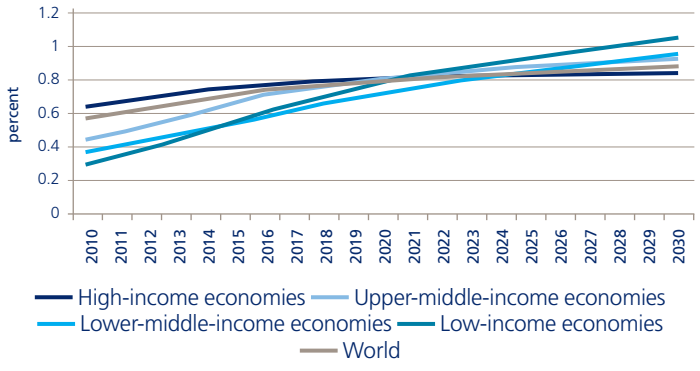
These costs are high, but still far below the costs of other global scourges. For example, the Institute for Economics and Peace *2015 Global Peace Index Report* estimated that the costs of sub-national and international violence in 2014 is around USD 14.3 trillion or 13.4 percent of world GDP.[15]

Figure 13: ICT cybersecurity spending, by World Bank country income group, percent of GDP, 2010-2030



Source: IFs 7.15

Figure 14: ICT cyber adverse event costs, annual total, by World Bank country income group, Percent of GDP, 2010-2030



Source: IFs 7.15

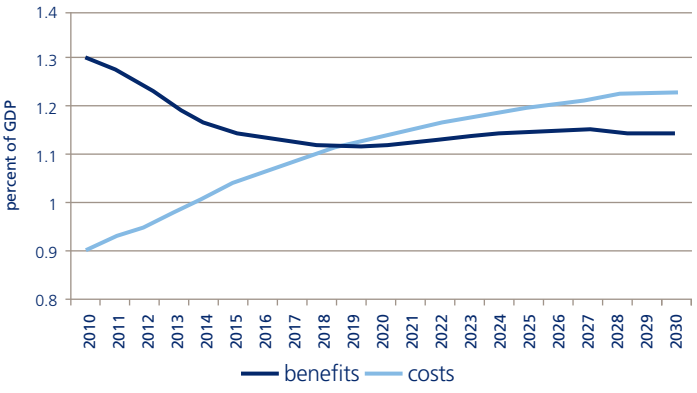
Comparing costs and benefits: the bad news

Figure 15 compares the global annual benefits and costs of ICT. Strikingly, it is not just theoretically possible that the annual **costs** of ICT security might outweigh the economic benefits of connectivity; in fact, such an inversion is projected to occur in the next few years, perhaps even before the year 2020, at somewhere near 1.1 percent of global GDP (roughly USD 1 trillion). While this finding is in line with our initial hypothesis, it was still surprising to see that this event is already expected to happen in the near future, according to our model.

This turning point calls attention to just how feeble cybersecurity has been in the face of ever more dangerous cyber-attacks. Either cybersecurity costs need to become far more effective (or significantly less expensive) or the benefits of ICT need to continue to multiply. Both of these potential futures are explored later in this report.

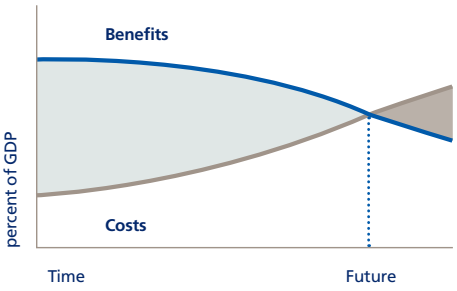
This conclusion has one very obvious caveat: both data and forecasting include a great many assumptions and estimates. The exact year of such a cross-over is highly uncertain, and perhaps it will never even occur, especially if the benefits or costs change significantly.

Figure 15: ICT cyber benefits and costs, global annual totals, 2010-2030



Note: Using 5-year moving average

Source: IFs 7.15



Comparing costs and benefits: the great news

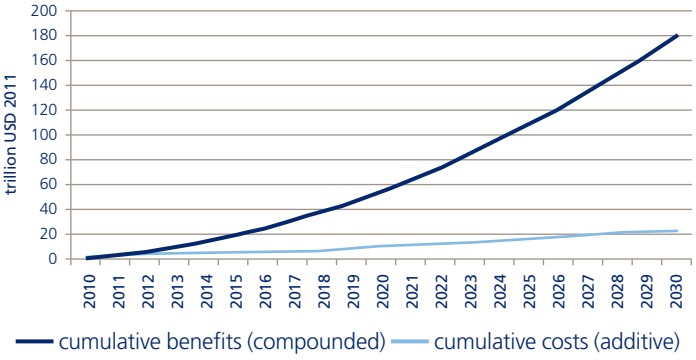
This report has already pointed out the difference in the way that the economic **benefits** of ICT accumulate over time (with a compounding effect as an investment) compared to the economic costs (as a simple sum of annual values). Figure 16 shows how this dynamic plays out to 2030: even in years when annual costs outweigh the benefits, compounding investments pay off over time.

On a global level, and for this conservative Base Case, the cumulative benefits between 2010 and 2030 are estimated to be about USD 180 trillion versus USD 23 trillion of costs (a net benefit of nearly 9 percent of the cumulative GDP between 2010 and 2030).

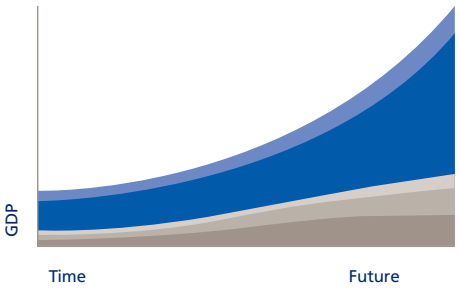
These costs are huge and demand the attention of policymakers, but they are dwarfed by the benefits.

Again, note how the actual modeled costs and benefits accumulated over time compares to the theoretical curve (inset).

Figure 16: ICT cyber benefits and costs, global cumulative totals, in USD trillions, 2010-2030



Source: IFs 7.15



Comparing costs and benefits: by economy and region

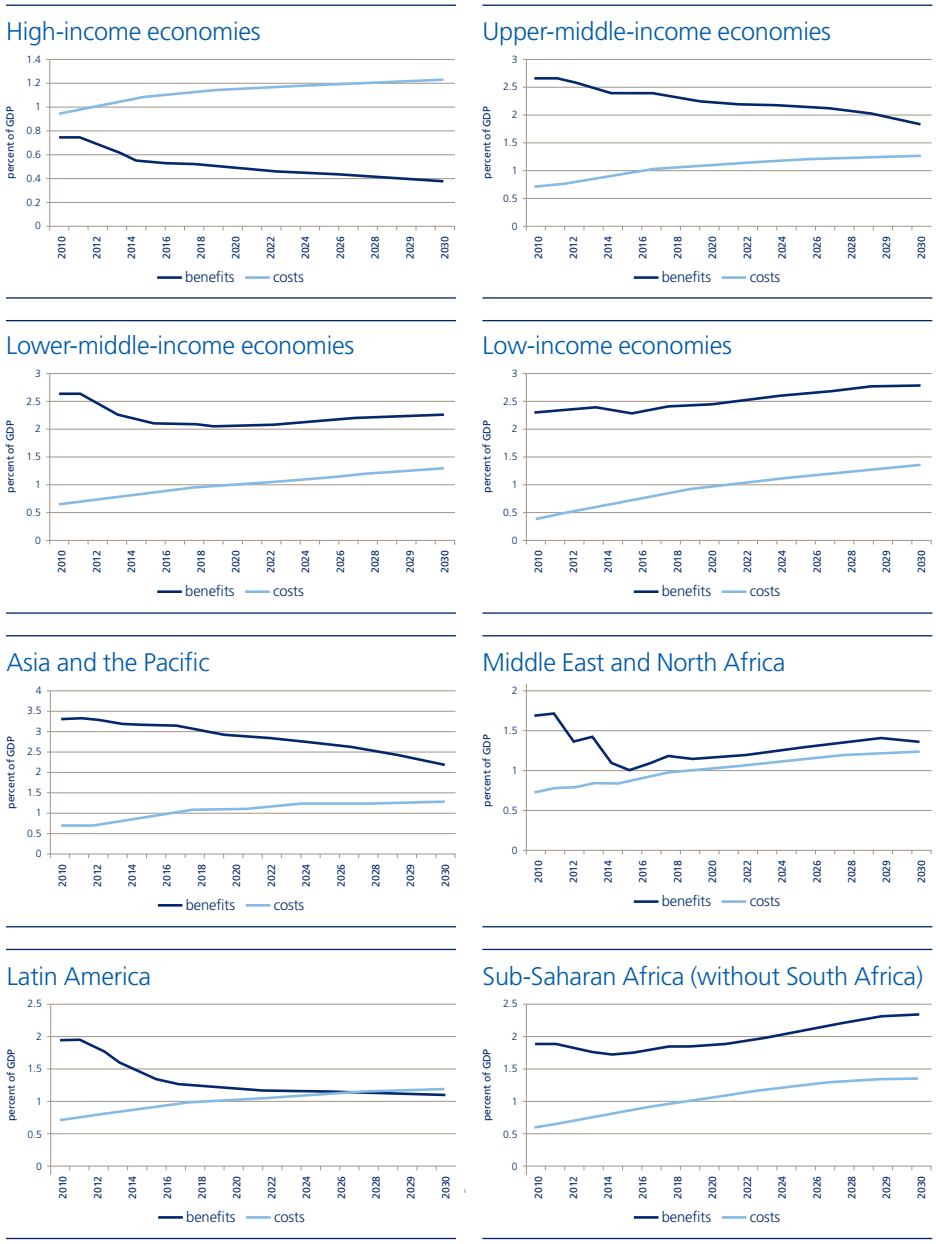
There is great variation of those patterns across country income groupings and regions (Figure 17).

The cost/benefit inversion point appears to already have been reached for high-income countries. In OECD nations, the annual costs of being connected may already outweigh the benefits. As noted above, this is because of the relative saturation of ICT in advanced economies in the face of steadily rising costs. New advances could, of course, freshen new waves of productivity (such scenarios are explored in the next section).

The inversion is likely to be approaching for upper-middle-income countries by roughly 2030, though it seems unlikely for low-income countries even by that time, as they are still able to add gains from ICT.

Among the developing regions shown in Figure 17, the process of likely convergence in annual benefits and costs is apparent in all but sub-Saharan Africa. The cross-over will probably occur in Latin America before 2030 as that region bridges the digital divide and in the Asia Pacific region sometime after that.

Figure 17: ICT cyber costs and benefits, annual totals, by World Bank country income group and World Bank region, percent of GDP, 2010-2030



Note: Using 5-year moving average

Source: IFs 7.15

Alternate worlds: exploring the future

The analysis so far has explored the Base Case, assuming that future trends are relatively consistent with or easily understandable from those in the past. For example, one of the dominant assumptions of the Base Case, borrowed from the ITU's ICT Development Index, is that the ICT wave will have largely played out by 2030 for both high-income and upper-middle-income countries, as they gain universal access to mobile and broadband technologies.

But, of course, the future is always sure to hold tremendous surprises.

One of the most useful tools for peeking over the horizon of time is a structured approach of formulating and analyzing 'alternate worlds,' differing futures based on the outcomes of major uncertainties. One of the most influential reports that explores alternate worlds is the *Global Trends* series from the U.S. National Intelligence Council (NIC).[16] Experts from both the Atlantic Council and Pardee Center were central to that effort and brought their experiences here to explore future cyber scenarios. Additional alternate worlds work has been done by Microsoft and CISCO in their reports, *Cyberspace 2025* (2014) and *The Evolving Internet* (2010), respectively.[17]

The first step is to identify the 'axes of uncertainty' that are likely to be most important. Over the course of this project, two such uncertainties clearly stood out.

The first major uncertainty is whether the globe continues to reap great benefits and keep the risks under control or whether hackers, nation-state attackers, and trolls greatly degrade the Internet and the benefits of being connected. We call the two distinct futures anchoring this dimension the *Cyber Shangri-La* and *Clockwork Orange Internet*, respectively. In the first scenario, secure Internet connectivity is a global right; in the second, it is a luxury good. As such, these scenarios alternately represent the most benefit and the highest cost.

The second uncertainty is whether the future Internet will be more dominated by governments (with strong borders and government monitoring) or the private sector (where the technological elite is constantly able to invent around government control). These are the *Leviathan Internet* and *Independent Internet* futures, respectively. Whereas *Cyber Shangri-La* is obviously a better scenario than the *Clockwork Orange Internet*, there is a more difficult balance here, which will be explored in later sections.

Alternate worlds: Cyber Shangri-La

Individuals can reach their full potential in Cyber Shangri-La.

Cyber Shangri-La is the future in which all of Silicon Valley's dreams come true. The unfettered development of ICT and global networking drives innovation and prosperity while helping individuals reach their full potential, regardless of their nationality or circumstance. Privacy remains relatively high. Secure and reliable access to the global network is a fundamental human right.

This scenario is similar to the Peak future in Microsoft's *Cyberspace 2025* report and the Fluid Futures in CISCO's *The Evolving Internet*.[18] All three describe a future situation where technological progress has continued, users have high levels of trust in the system, and companies continue to build out the network and connected devices.

Dynamics: Costs remain flat or only rise slightly, while benefits rise rapidly or even exponentially. These changes occur modestly, with steady changes over time.

Most if not all of the twelve game-changing technologies, identified by McKinsey Global Institute (see Box 2 on page 11), deliver on their full promise, especially those most dependent on strong cybersecurity: mobile Internet, automation of knowledge work, IoT, cloud technology, advanced robotics, and autonomous and near-autonomous vehicles.

New technologies boost benefits far, far faster than costs accumulate. Defense has become easier and cheaper than offense, so that costs remain modest and stable. For example, perhaps autonomous or autonomic defenses are widely deployed, moving significant attacks out of the range of all but the most capable and motivated adversaries. Defense improving faster than offense is a critical enabler for unlocking full economic and societal benefits.

Impact on the economy: ICT is a main driver of global innovation across all economies, with high degrees of globalization as the Internet becomes increasingly ubiquitous, secure, and resilient. ICT benefits among nations converge, as most netizens and companies around the world have access to similar kinds of technologies. Global cooperation on cybersecurity is relatively high, though nations still have strong disagreements over cross-border content.

Impact on individuals: People have widespread and well-founded trust in the technologies, providers, and behavior of other netizens. Their online persona is fluid, sometimes tied to their national identify but at other times tied to any other association, state or non-state, that they choose. Privacy is well within each individual's control.

Alternate worlds: Clockwork Orange Internet

Hackers tear down security defenses in the Clockwork Orange Internet.

The worst nightmare of anyone who is connected, the *Clockwork Orange Internet* is almost entirely made up of ultra-violent 'bad neighborhoods,' akin to the novella and cult-classic movie of the same name. Secure and reliable access to the global network is no longer a global right but a luxury good. Digital identities and assets huddle behind high walls. Technology still advances, but without necessarily being networked; high-tech is no longer synonymous with information tech.

Dynamics: Cyber offense is no longer just better than defense, it is unbeatable. Any time new security initiatives and projects are launched, there are nations, hackers, or curious security researchers who quickly tear them down. Cyber bullying and other bad behavior is rampant. There is little to no trust, as people cannot have faith in their networked devices or other people online. This lack of trust is both a cause, as well as a symptom, of massive cyber sub-prime cascading failures across the Internet and into connected infrastructures. ICT usage is so choked down that even technologies that were common in 2015 (such as online shopping and social networking) are reserved only for those rich enough to pay for proper security.

Impact on the economy: Costs rise rapidly while benefits only rise slightly. Networked ICT becomes a drag to the economy. Disruptions most heavily affect higher-income economies and the most ICT-saturated middle economies. Lower-income economies don't suffer these costs, but also receive far fewer gains. Globalization is mostly broken, and companies find it hard to make a profit selling IT, except as a luxury good.

The negative effects could happen either steadily ('ice' scenarios), or very quickly ('fire' scenarios). The 'ice' scenarios include steadily increasing costs over time, such as the continued worsening of cybercrime, crises and conflict (including international conflict), and a general breakdown in governance. The 'fire' scenarios include fast-moving events, such as a major conflict, global shock, or sudden and unmatched offensive innovation.

This leads to high degrees of ICT inequality, as only large multinationals and other dedicated firms can afford security. The rich around the world can still use secure ICT, but for most others, it is simply out of reach or only usable at great risk. Governments, the finance sector, and others have built a secure minimum essential information infrastructure, which is as difficult to enter as a U.S. federal government building, and only available for the most secure purposes. There is also very little international cooperation, with little trust between nations who attack each other (and each other's products) relentlessly.

Impact on individuals: Online persona becomes a thing of the past for most people. People have only as much trust as their credit cards can buy, while an online identity is an asset to flaunt in the best circles. Privacy is no longer a primary concern, now that connectivity itself is a risk.

Alternate worlds: Leviathan Internet

Some nations monitor their citizens closely in the Leviathan Internet.

In the *Leviathan Internet*, there is no longer a single global Internet but a series of national internets dominated by sovereign governments (and particularly their national security apparatuses). Information technologies are more useful to governments to keep track and control over citizens than vice versa.

Dynamics: Some nations, like Russia and China, choke off their national borders so that all information – and attacks – has difficulty penetrating. They rely on heavy monitoring of their networks to keep an eye on their citizens and control what information they receive, using technologies that help to stop many attacks. Other nations, including most in the OECD, have more open national borders and suffer comparatively more attacks.

Cybersecurity decreases overall. The small benefits brought by strong regulation and national borders are more than offset by decreased global cooperation and increased cross-border espionage, sabotage, and conflicts.

Impact on the economy: The impact on the economy is modest, with continuing growth of GDP and productivity, but well below the dreams of tech visionaries. Cross-border restrictions undermine too many technologies, and tight regulations limit innovation. Protectionism trumps globalization, with nations giving preference to their own companies and insisting on ICT localization and sovereignty, shattering the global ICT market. There is little trust even between friendly nations, as policies are driven more by security fears than dreams of innovation.

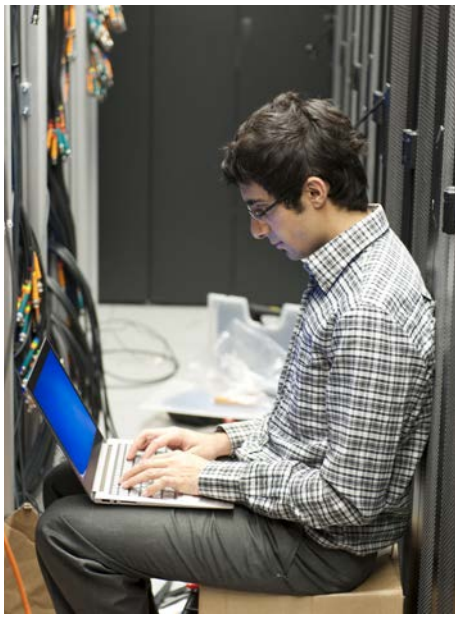
Some nations close off their national borders to all kinds of information, from unpleasant news to damaging cyberattacks. Other nations, including most OECD states, are slightly more porous. ICT inequality accordingly increases, with big nations and blocs like Brazil, China, the U.S., and the European Union having enough scale to succeed. Smaller nations struggle to build enough sovereign infrastructure. By 2030, this process of speciation is so far along that these separate internets, despite their once common ancestor, can no longer interconnect.

There may be gradients and variants of the *Leviathan Internet*, such as:

- 'Huntington Internet,' in which different cultures have different Internets;
- 'Iron Curtain Internet,' in which different Internets exist for Western nations and more closed societies like China and Russia; and
- 'Schengen Internet,' in which different trade blocs have their own 'free exchange' of bits and bytes.

Impact on individuals: People's online personas are driven by their country of residence. Online trust is high for those that trust their government but low for everyone else, and non-existent across borders. While there is nearly zero privacy from governments, there are very tight restrictions on the commercial use of similar data.

Alternate worlds: Independent Internet



Cyber-experts have more power in the Independent Internet.

In the *Independent Internet* scenario, governments are unable to regulate and dominate this new technological space. Compared to today (and the assumptions in the Base Case), non-state actors have bloomed into the true online powers. As proclaimed in 1996 by John Perry Barlow, a noted cyber-libertarian and former songwriter for the Grateful Dead: "Governments of the Industrial World, [y]ou have no sovereignty where we gather... Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."[19]

Governments still try to pass regulations, but are quickly left behind by the true cyber powers: companies, non-state groups, individuals, and regions (not least Silicon Valley). The technological elite defy the state and continue to invent new ways to outfox regulations, laws, and other constraints of the state, such as refusing requests for government backdoors. This private-sector domination keeps benefits coming steadily but generates insufficient breakthroughs on defense.

Dynamics: Offense still maintains the advantage. ICT companies continue inventing new defenses, but without effective policing and control, criminal groups continue to thrive. Large companies increasingly apportion more of their 'security' budget for offensive means to disrupt incoming attacks or seize back their stolen intellectual property; there is a concomitant rise of cyber-Blackwaters (private defense companies) to help companies actively disrupt their tormentors.

Likewise, high-end attacks and espionage are not just the purview of China or the U.S., but are 'democratized' to include companies and super-empowered individuals. Trust is accordingly modest; while it can be high within different corporate walled gardens (for example, Apple users would tend to trust Apple and other Apple users) or social groups, it is missing at higher levels. ICT equality and globalization are also high, as most netizens and companies all over the world have access to similar kinds of technologies.

Impact on the economy: Networked ICT is an important driver of innovation, productivity, and GDP. Income inequality is likely to increase. The effects are relatively broad but somewhat favor higher-income economies. There are high degrees of globalization as national borders are unable to fence out foreign companies, technologies, or information. However, there may be walled gardens, as people get locked into one alliance of technologies versus another (such as Apple, Facebook, Microsoft, Google, or Baidu) and can change their alliance only with great difficulty. These companies may develop into a relatively stable arrangement (like a Gang of Four or Big Five) or they may change over time.

Impact on individuals: People do not tend to see their online personas as 'American' or 'Brazilian' but as a member of a particular technology alliances. Once you are an 'Apple' or 'Google' person, that identity remains relatively stable. Online trust is somewhat higher than in the Leviathan Internet because of widespread encryption and other measures. Individuals tend to have very high privacy vis-a-vis governments, but have opted-in to relatively intrusive monitoring by the companies with whom they choose to do business.

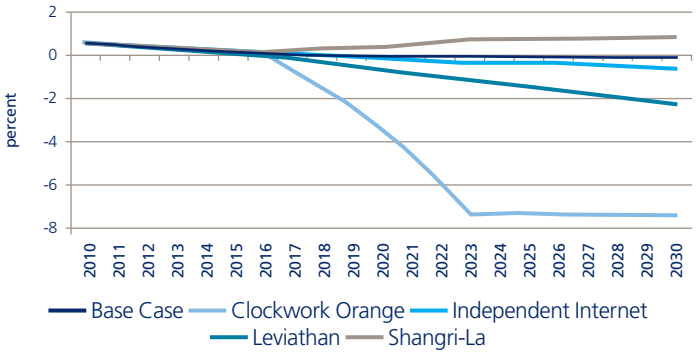
Costs and benefits in alternate worlds

In the Base Case presented in the first half of this report, there was already great uncertainty underlying the data and forecasting. These uncertainties are therefore magnified when looking at alternate future cyber worlds. But the trend is the most important factor to take into account, and the shape of the curves tells a compelling story.

In the *Clockwork Orange Internet* scenario, the attackers don't just have the advantage over defenders; true supremacy induces a net cost drag of nearly 7 percent of global GDP by 2023. The reason for the plateau in those net costs is the assumption that there is a 'saturation of catastrophe,' where things cannot get worse.

The net annual economic benefits in the *Cyber Shangri-La* scenario over the Base Case might look small, but in fact would represent a reversal of the current trend toward an overall net negative effect. And in the *Leviathan* future, governments looking to separate their ICT innovations and connections from those of other countries should be cautious, as strong Internet borders could shift net annual costs above benefits by a full 2 percent of GDP by 2030. The net loss in the *Independent Internet* is far smaller, but still negative, at a fraction of one percent.

Figure 18: ICT cyber net benefits or costs, global annual total, as a percentage of GDP, by scenario, 2010-2030



Source: IFs 7.15

> The wide range of forecasts illustrates the very considerable uncertainty we face."

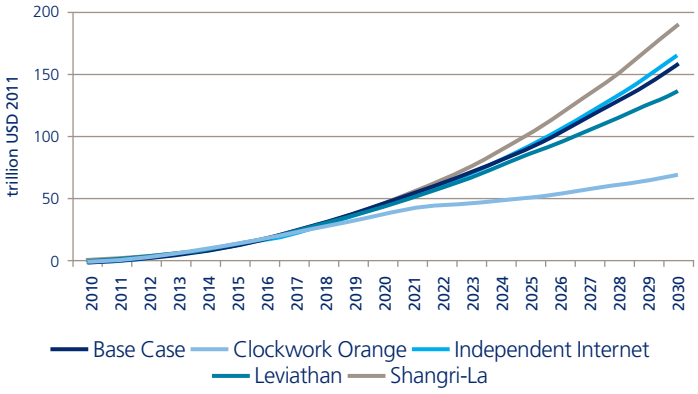
The implications of these differences among alternate worlds become more obvious and pronounced when costs and benefits are compared on a cumulative basis over time, rather than just annually.

The compounding investment and productivity impacts from ICT in *Cyber Shangri-La* mean that even the scenario's very modest net annual benefits result in a cumulative net contribution that is perhaps USD 190 trillion, USD 30 trillion higher than the Base Case by 2030. For context, the total cumulative GDP of the Base Case between 2010 and 2030 is forecast to be USD 2,000 trillion, so that the net benefit of ICT in *Cyber Shangri-La* begins to approach 10 percent of that long-term GDP.

The worst case of a *Clockwork Orange Internet* might cost the world nearly USD 90 trillion of potential net economic benefit across the period to 2030, when compared to the Base Case, and USD 120 trillion relative to the best case of *Cyber Shangri-La*.

The *Independent Internet* is very close to the Base Case, but the *Leviathan Internet* of strong national borders drops cumulative ICT net benefit by USD 20 trillion relative to the Base Case. Overall, the wide range of forecasts across these scenarios illustrates the very considerable uncertainty we face concerning both benefits and costs in cyberspace.

Figure 19: ICT cyber net benefits or costs, global cumulative total, in USD trillions, by scenario, 2010-2030



Source: IFs 7.15

Implications for 2020 and 2030

Deciding how to steer between alternate futures to guide policy often results in a very basic problem of political philosophy worthy of Hobbes, Locke, and Rousseau: is it better to avoid the worst cyber futures or to aim for the best? Of course, we want the best cyberspace for ourselves and our children, but when humanity has aimed for heaven, then missed, we have often wound up in hell.

It is not a tough decision whether a *Cyber Shangri-La* or a *Clockwork Orange Internet* future is preferable; the latter has few redeeming features to anyone but a pure technophobe. Policymakers might choose to aim for *Cyber Shangri-La*, where the benefits far outweigh the costs, but they certainly need effective policies to avoid the *Clockwork Orange Internet*, with USD 90 trillion less in global net benefit from ICT than even that of our conservative Base Case. Even if the trends are correct, but are off by an entire order of magnitude, the loss is still nearly USD 10 trillion.

It is not as easy to judge between the points on the other axis of uncertainty, which is between the roles of governments versus non-state groups. The modeling shows more economic benefits, up to USD 20 trillion, if states keep their hands off the cyberspace, but that reflects a particular set of assumptions – that borders will hurt more than they help. It would be easier for nations to monitor their own (or others') citizens, undermining trust in the system, or to disconnect themselves (or their adversaries) from the Internet altogether. Government regulation might limit innovation for little or no actual security benefit.

Which futures seem to be more likely today? During the course of this research, countless experts made gloomy projections for the next five years.

Cyber risks will continue to rise significantly in the near future. Technological and process innovation might help some organizations, but overall there is little on the immediate horizon that suggests that cyberattacks will become less common. With the massive profusion of recent tension between major military powers, the trend is perhaps more towards a *Clockwork Orange* or *Leviathan Internet*.

Cyberattacks might get much worse, far more quickly than many risk managers and policymakers may be expecting. At first, it may be difficult to determine the trajectory we are on, because projections for the alternate worlds are not that different in 2016 or 2017. If cyber-incidents continue to grow steadily, then it is likely that we are heading towards *Clockwork Orange Internet*, meaning immediate costs that exceed benefits by 1.5 percent of GDP each year, a gap that could rapidly grow larger.

In the U.S., it has been said the theft of intellectual property has been the greatest transfer of wealth in history, but this looks like small change compared to the total costs – and potentially much more deleterious futures ahead.

The individual cyber events we experience on a daily and weekly basis and the costs we pay to limit them are aggregating over time and could have a far larger negative impact than most realize: a cumulative sum of USD 23 trillion even in the Base Case and as much as USD 109 trillion through 2030 in the *Clockwork Orange Internet* future. The Internet can and will change over time, leaving the world with an Internet that may be far less resilient than the one we have today, an Internet that is no longer an engine of innovation and growth.

These would be horrendous economic costs, which the world cannot afford and, if we take smart action now, need not pay.

The resulting damage costs the U.S. economy USD 243 billion under a milder scenario and as much as USD 1 trillion in the most extreme scenario."

Box 3: What if the U.S. suffered a cyber-disaster?

The Stuxnet Worm was perhaps the first cyber-attack on a country that caused physical damage to infrastructure – and while the virus was highly targeted on Iran's nuclear facilities, a next-generation worm might be able to cripple critical infrastructure networks across an entire country.

Imagine: sometime in the near future, a cyber-worm spreads through the U.S.'s critical infrastructure networks, targeting the software control systems of electrical stations, transportation and communication hubs, water treatment stations, etc. The attack results in massive power and Internet outages, crashes mobile networks, disrupts water supply, shuts down the country's air traffic, and more. What might be the economic cost of such a severe disruption?

While we have no historical examples to draw from, the insurer Lloyd's of London has developed a hypothetical scenario of a large-scale cyber-attack on the U.S. electrical power grid in order to gauge the economic costs of such an attack.[20] In their scenario, a piece of malware spreads through much of the Northeastern U.S. grid, infecting the software controlling generators and causing them to overload. The physical damage inflicted by the malware results in power outages affecting 93 million people across fifteen states that last anywhere from twenty-four hours to several weeks.

The resulting damage to infrastructure, lost business revenues, supply chain disruptions, transport and water network disruptions, etc., costs the U.S. economy USD 243 billion under a milder scenario (outages last two weeks, fifty generators damaged) and as much as USD 1 trillion in the most extreme scenario (outages last four weeks and 100 generators damaged).

The Lloyd's report provides some important takeaways: (1) the economic costs associated with a cyber-induced infrastructure outage are "non-linear with respect to the size and duration of the outage;" (2) with a severe initial shock, the impact to GDP tends to disappear within three to four years of the attack; (3) imports and exports are particularly impacted due to transport disruptions – the scenarios assume a 100 percent shock to exports compared to a 50 percent drop in labor productivity and consumption for the duration of the outage.

Singapore's connectedness means it is more vulnerable; its strength as a 'smart nation' has its downsides."

Box 4: How does cybersecurity affect prosperity and innovation?

There appear to be at least four general mechanisms by which cybersecurity directly underpins economic growth. It:

1. enables specific innovative technologies, such as the IoT;
2. protects intellectual property, the source of innovation, from being stolen and copied;
3. precludes direct costs from cyber-crime and the response to malicious incidents; and
4. prevents disruption to the digital economy, since a digitized economy requires digital security.

Signposts for the Better Futures

1. General improvements in global governance (such as at the United Nations, G20, and Internet Corporation for Assigned Names and Numbers (ICANN)), reducing costs and increasing benefits
2. Collaboration between the U.S. and China or the West and Russia, which again reduces costs and increases benefits, maintaining international standards, creating less protectionism, and resulting in fewer cyber conflicts
3. New sub-waves of ICT keep the benefits booming with major new disruptive technologies, such as cloud computing, quantum computing, IoT, and artificial intelligence
4. Disruptive defensive technology gives defenders the edge, thus reducing costs

Signposts for the Worse Futures

1. Increasing conflict between the U.S. and China and between the West and Russia
2. Failures in international governance and continued breakdown of nation-states
3. New disruptive offensive technologies gives attackers supremacy, causing costs to rise suddenly and dramatically
4. Unseen feedback mechanisms allow failures or attacks in one part of the system to spiral far further and more quickly than expected

If we're going to build a global and secure internet moving forward, China and Russia will have to be more involved."

Notable ideas from participants

"Only a catastrophic cyber shock would lead a potential global alliance of countries and companies and individuals to come up with a new, secure system with high standards. How many wake-up calls do you need to make it a shock?"

Participant in Abu Dhabi

"Singapore's connectedness means it is more vulnerable; its strength as a 'smart nation' has its downsides. Even [well-run] Singapore has trouble managing all the infrastructure and services connected with being a regional data hub."

Participant in Singapore

"Even though the 'splinternet' is an old concept, it has potentially increased relevance for Asia; in the region, the focus on cyber sovereignty is a likely cyber future. China seems increasingly bent on edging out US companies in favor of only increasingly pliant Chinese companies that the government can control."

Participant in Singapore

"Brazil will keep the Internet growing as Western developed nations slow down their use of the Internet and get mired in a discussion of legalities. It is likely that Brazil and other emerging countries, if guided by Western expertise, can help determine the path on how data is treated internationally and establish norms for the future."

Participant in Sao Paulo

"If we're going to build a global and secure internet moving forward, China and Russia will have to be more involved. If not, like-minded nations will have to come together and create a different space."

Participant in Montreal

Implications and recommendations for companies

The main hope for companies in any of the cyber futures remains resilience."

To think of ICT and cybersecurity in financial terms, companies are all 'long' on ICT, having essentially bet the future of the franchise that the benefits of being connected will not wreck the firm should there be a massive outage, collapse, or attack. Sony Motion Pictures, Target, and other companies showed the downsides of such a position without much of a hedge. We start with the more basic recommendations, focused internally and technically, then move farther up.

Start by taking care of the basics: build a solid cybersecurity foundation by **implementing the top twenty controls** published by the Council on Cybersecurity, especially application white-listing, standard secure configurations, reduction of administrative privileges, and a quick patching process.[21]

According to Gerry Kane, Risk Engineer for cybersecurity at Zurich Insurance Group, "'set-it-and-forget-it' solutions are a thing of the past, as effective security requires constant vigilance, monitoring, and proactive hunting for threats already on your network." He says, "the most effective organizations know exactly where their data is, where it goes, and how it gets there. They encrypt it whenever possible or build other layers of control. The not-so-good ones are those who make a point of telling us they are compliant to some standard and then recite those controls that are the minimum required."[22]

In the spirit of this report, companies should use **metrics to help determine the cybersecurity return on investment**. As expressed by one participant in this report, Neal Pollard, Nonresident Senior Fellow at the Atlantic Council's Cyber Statecraft Initiative, companies should invest in cybersecurity to extend the interval between adverse cyber events and decrease the intervals to effective detection, response, and recovery, once breached.[23]

According to Richard Bejtlich, Chief Security Strategist at the cybersecurity company FireEye, "the median amount of time from an intruder's initial compromise, to the time when a victim learns of a breach, is currently 205 days."[24] Companies that can bring this metric down to 100 days, or ten, or even one will minimize the costs of adverse cyber events, likely disproportionate to their investment in such measures (and avoid reputational issues and CEO or board-member resignations). The Cyber Green Initiative, initially funded by the Japanese Computer Emergency Response Team, is working to use similar measurements to collaboratively help 'clean' the cyber environment.

In all except the best future outlined in this report, cybersecurity problems will only get worse. In these scenarios, prevention is necessary, but not sufficient. The main hope for companies in any of the cyber futures remains **resilience**, the ability to bounce back from disruptions to make them as short and limited as possible. Redundancy, incident response, business continuity, scenario planning, and exercises will all help to make companies more resilient.

Three other recommendations from the April 2014 report by the Atlantic Council and Zurich Insurance Group, *Beyond Data Breaches: Global Interconnections of Cyber Risks*, are worth repeating here:

- **Push accountability for cyber risks**, starting with board-level cyber risk management. Cyber risks could bankrupt companies, so companies must include a broad view of global aggregations of cyber risk in their risk registers, hold executives accountable, and move away from a checklist/ audit perspective.
- **Get insured.** With cyber insurance, companies can transfer cyber risks, especially for third party risks associated with data breaches or business interruption.
- **Extend the horizon of risk management** to counterparties, contract and outsourced partners, and upstream infrastructure. For example, one financial institution reviewed every contract and outsourcing agreement, rating the criticality of each, and auditing those on which they had the most exposure.

The findings in this report also suggest that risk managers and corporate strategists **consider worst-case cyber futures** when looking at business strategies that are heavily Internet-dependent (and of course it is hard to find a business strategy that is not). According to the models examined in this report, even in the relative short term, by 2018, there could be damage from massive cyberattacks equivalent to 1.5 percent of global GDP. This is certain to drastically increase risks and drag down net profits for companies that are most exposed to cyber-attacks.

Nations are also likely in the near term to impose more sovereign boundaries on the Internet, which might force companies to develop separate business plans and ICT infrastructures for different internet blocs.

These steps, which are nearly entirely all internal actions for a company, fail to completely protect against the worst cyber futures examined in this report, which affect the global economy as a whole. It is therefore also necessary for companies to **engage with policymakers** to help drive towards the better futures.

One way to engage is through normal lobbying and industry groups. But companies should also band together to influence the Internet governance process. Non-ICT businesses – which will, after all, probably bear the majority of costs and enjoy the majority of the benefits – are probably under-represented in Internet governance forums, compared to nations, ICT companies, civil societies, or even individual technologists or former politicians. Increasing business representation might help keep resilience and security at the forefront of governance conversations.

Implications and recommendations for policymakers

The best solutions will be those with a focus on scale and those that can remove entire classes of attacks."

This tension between state and non-state solutions is a general trend and not confined to cyberspace, as noted by Barry Pavel and Peter Engelke of the Atlantic Council: "More power is spreading to more nation-states, leading to a more complex interstate system [and] more power is accumulating in more peoples' hands, leading to greater challenges to state preferences and capabilities as well as to the basis of the international system itself."[25] Pavel and Engelke call this world 'Westphalian Plus' to highlight the fact that non-states have more power on the global stage, sometimes approaching that of nation-states, the modern idea of which was established by the Treaty of Westphalia in 1648.

Instead of aiming for any of the extreme ends of the two axes of uncertainty that are included here as alternative futures, policymakers might aim for an intermediate situation that Pavel and Engelke call a **strategy of dynamic stability**.[26] In this scenario, a strong and resilient Internet is driven by a healthy non-state sector, supported when needed by governments. At this point, non-state groups can drive innovation and respond with agility to security incidents, but also draw on government support, which have a larger wealth of resources, longer endurance, and access to other levers of power.

Achieving dynamic stability is a global collective action problem that requires a **sense of joint stewardship** over the Internet. Internet governance accordingly needs a larger scope, moving away from a focus on determining who runs specific technical functions to ensuring sustainability, so that the future Internet continues to be a global source of wonder and innovation for decades to come.

Instituting large-scale surveillance or erecting Internet borders might be seen as unsustainable practices, just as at odds with the future as clear-cutting tropical forests or emitting endless CO_2. It would further open new options borrowed from the environmental sustainability concept, perhaps snapping the discussion out of the unproductive deadlock of security versus privacy.

Cyber stewardship might mean, for example, an Internet governance focus on collective action in the face of major Internet outages or attacks. During the 2008 financial crisis, the governance mechanism included the International Monetary Fund (IMF), the G8 grouping of nations, and the Bank for International Settlements in Basel, Switzerland. None of these mechanisms exists for fast-moving cyber shocks. Borrowing an idea from Microsoft, the earlier *Beyond Data Breaches* report by the Atlantic Council and Zurich Insurance Group discussed the possibility of a G20+20 group (comprised of the largest economies together with the twenty most systemically critical ICT companies) to handle this governance problem.

Even though this is a collective action issue, not all actors are equal. High-income economies, like the U.S., member states of the European Union, Japan, South Korea, and Taiwan, are the most heavily dependent on ICT and accordingly have the most to lose in the face of the cyber risks described in this report. **Therefore, high-income economies especially should commit to increased funding and cooperation on governance, and demonstrate exceptional caution in using the Internet for intelligence and military purposes**.

This cooperation should include discussing the projections in this report with developing countries and together **building capacity** so that they can avoid the worst cyber security problems that plague high-income countries. Such sharing may also help to build an international consensus on fighting cybercrime. For maximum effectiveness (and economic benefit), such assistance should not just go to governments to build emergency response teams or develop cyber-crime laws, but also to non-state groups to nurture a local cybersecurity industry.

Policymakers should continue to **encourage next-generation security projects**, but should not expect them to save the day. It may not be possible to re-design a new, more secure Internet, though there are technical efforts that aim to do so.[27] Likewise, it is probably too late to 'bake-in' security to the IoT; too many insecure devices have already been deployed to consumers and companies.

The best solutions will be those with a focus on scale and those that can remove entire classes of attacks. Recently, the Atlantic Council informally surveyed a group of cybersecurity experts about what innovations of the past decades had most significantly protected computers from cyber-attacks. The answers, including the launch of Microsoft's Windows Update to simply update computers with more secure software, had one thing in common: they could easily be scaled so that one relatively inexpensive action protected millions or billions of computers. Newer technologies similarly use scale to asymmetrically aid defense. For example, multi-compilers accomplish the equivalent of mixing up the 'genetic diversity' of programs, so every version is different enough that attackers cannot simply re-use their intrusion tools again and again. They must modify those tools for every single copy of the software.

Investments in the overall stability, governance, and resilience of the system are instead the better option, and are likely to be repaid many times over. Based on the modelling done for this report, by 2030, investments such as more secure Internet standards, a more robust Internet backbone, and an effective multi-stakeholder governance model could yield global economic benefits of hundreds of billions, if not trillions, of dollars.

National policymakers also should **encourage cross-border digitized trade and avoid location-specific policies** (that emphasize where data is held; so called 'data localization') **or market restrictions** on where ICT equipment is made. Even if such protectionist market restrictions make policy sense in the short run, they import physical borders, which will similarly reduce trade and hurt national and global GDP growth. An excellent project along these lines is the E15 Initiative, co-run by the World Economic Forum, which has a task force to seek "improvement in the global trade system to enhance economic benefits from the digital economy."[28]

As importantly, national borders are likely to lead to a more brittle Internet, as ICT companies that build and maintain cyberspace are forced to answer to dozens of national regulators and build local infrastructure to meet different local laws. Resilience is no longer a shared concern subject to multiple global stakeholders, but a national concern, subject to bureaucrats and leaders who are not always democratically elected or have their citizens' best interests in mind.

Conclusion

This project began by exploring a critical risk management question for the twenty-first century: how would we know if the risks of being connected, whether those risks have been realized or not, are starting to outweigh the benefits?

After interviews around the globe, extensive research, and economic modeling, it now seems obvious that, on an annual basis, the benefits of ICT to global GDP will be outweighed by the annual cybersecurity costs. Fortunately, because the benefits tend to be investments that compound over time, they will continue to outpace the costs, even in the worst possible futures.

Yet tens and even hundreds of trillions of dollars are at stake, nearly 10 percent of total global GDP, not to mention the social and cultural impact of ICT. Most of the experts consulted for the report were not optimistic about our future, with a consensus that the trends were heading in the wrong direction. These trends may be approaching a tipping point, with perhaps a small window of a few years to pull back and reorient towards a more secure and more resilient Internet. The decay of trust among all parties and the deteriorating global security situation will make solutions much harder.

Companies must start preparing for an Internet that may be far less business-friendly, with more sovereign borders and more disruptive attacks. Addressing cyber risks is an issue for corporate boards, not the IT department. National policymakers must treat the Internet as a global resource that can be depleted like any other and that requires stewardship if it is to remain productive.

If we cannot create a more sustainable cyberspace, then it will likely be far less safe, secure, and resilient for future generations than it has been for ours.

For more details on the model, data, and process used in this report, please see and use the IFs model at http://www.pardee.du.edu, find the companion report produced by the Denver University's Pardee Center for International Futures at http://www.pardee.du.edu/cyber-benefits-and-risks-quantitatively-understanding-and-forecasting-balance, and use the dashboard for simplified computer or mobile device analysis of our forecasts at http://www.ifs.du.edu/ifs/frm_CyberDashboard.aspx

About us and this report

About **Zurich Insurance Group**: Zurich Insurance Group is a leading multi-line insurer that serves its customers in global and local markets. With about 55,000 employees, we provide a wide range of general insurance and life insurance products and services. We serve individuals, small businesses, and mid-sized and large companies, including multinational corporations, in more than 170 countries.

About the **Atlantic Council**: The Atlantic Council is a Washington DC-based think tank promoting constructive leadership and engagement in international affairs based on the Atlantic Community's central role in meeting global challenges. The Council provides an essential forum for navigating the dramatic economic and political changes defining the twenty-first century by informing and galvanizing its uniquely influential network of global leaders. Through the papers we write, the ideas we generate, and the communities we build, the Council shapes policy choices and strategies to create a more secure and prosperous world.

About the **Frederick S. Pardee Center for International Futures**: The Pardee Center's mission is to explore, understand, and shape alternative futures of global change and human development. As part of this pursuit, the Center has built the International Futures (IFs) model, the most sophisticated and comprehensive forecasting modeling system available to the public. IFs uses our best understanding of global systems to produce forecasts for 186 countries to the year 2100. The Pardee team prepared a much more extensive technical report in support of the analysis, available here: www.pardee.du.edu.

Jason Healey of the Atlantic Council is the primary editor of this report, while **Barry Hughes** of the Pardee Center oversaw the team that conducted the modeling and wrote the resulting findings.

Other team members who were critical to the report and overall project include Barry Pavel, Mathew Burrows, Carles Castello-Catchot, Klara Tothova Jordan, Aparajitha Vadlamannati, and Anni Piiparinen from the Atlantic Council, and David Bohl, Mohammod Irfan, Eli Margolese-Malin, and José Solórzano from the Pardee Center.

End notes

[1] The names for these two alternate futures, Shangri-La and Clockwork Orange, were chosen as they are both fictional works from the past century. Each vibrantly illustrates a different world, one utopian and balanced, the other deeply dystopian. The book *Lost Horizons*, by James Hilton, about a mystical Himalayan paradise whose inhabitants live nearly forever was written in 1933; *A Clockwork Orange* was first a 1962 book by Anthony Burgess, but became a cult hit in the 1971 movie of the same name by Stanley Kubrick.

[2] Daniel E. Geer, Jr. "Cybersecurity and National Policy" (Harvard Law School National Security Journal, 2011), http://harvardnsj.org/2011/01/cybersecurity-and-national-policy/.

[3] Barry Hughes et al., "Cyber Benefits and Risks: Quantitatively Understanding and Forecasting the Balance" (Frederick S. Pardee Center for International Futures, 2015).

[4] Daniel E. Geer, Jr. "Measuring Security," http://geer.tinho.net/measuringsecurity.tutorial.pdf.

[5] McKinsey Global Institute, "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy," May 2013, http://www.mckinsey.com/insights/business_technology/disruptive_technologies.

[6] McKinsey Global Institute, "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy," May 2013, http://www.mckinsey.com/insights/business_technology/disruptive_technologies.

[7] National Security Telecommunications Advisory Committee, "NSTAC Report to the President on the Internet of Things," undated draft from 2014, http://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf.

[8] Moore's Law describes a prediction that the number of transistors (a computer's electrical switches representing 0s and 1s) that can fit on a silicon chip will double every two years as technology advances. This leads to incredibly fast growth in computing power without a concomitant expense and has led to laptops and pocket-size gadgets with enormous processing ability at fairly low prices; Annie Sneed, "Moore's Law Keeps Going, Defying Expectations" (Scientific American, May 19, 2015), http://www.scientificamerican.com/article/moore-s-law-keeps-going-defying-expectations/.

[9] David Wilkofsky, Arthur Gruen and Norman Eisenberg, "TIA's 2014 – 2017 Market Review & Forecast" (Telecommunications Industry Association, 2014), http://test.tiaonline.org/resources/market-forecast.

[10] David Wilkofsky, Arthur Gruen and Norman Eisenberg, "TIA's 2014 – 2017 Market Review & Forecast" (Telecommunications Industry Association, 2014), http://test.tiaonline.org/resources/market-forecast.

[11] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime," Economic Impact of Cybercrime II (Center for Strategic and International Studies, June 2014), http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

[12] Jessica Rettig. "What is the 'Base Case' Forecast?" (Frederick S. Pardee Center for International Futures, 2014), http://pardee.du.edu/news/what-base-case-forecast.

[13] International Telecommunication Union, "Measuring the Information Society Report" (United Nations, 2014), http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf.

[14] Beau Woods, email with Jason Healey, 3 July 2015.

[15] Institute for Economics and Peace, "2015 Global Peace Index Report," June 2015, http://economicsandpeace.org/wp-content/uploads/2015/06/Global-Peace-Index-Report-2015_0.pdf.

[16] National Intelligence Council, "Global Trends," http://www.dni.gov/index.php/about/organization/national-intelligence-council-global-trends.

[17] Microsoft, "Cyberspace 2025," June 2014, https://www.microsoft.com/security/cybersecurity/cyberspace2025/; CISCO, "The Evolving Internet," August, 2010, http://newsroom.cisco.com/dlls/2010/ekits/Evolving_Internet_GBN_Cisco_2010_Aug.pdf.

[18] Microsoft, "Cyberspace 2025," June 2014, https://www.microsoft.com/security/cybersecurity/cyberspace2025/;. CISCO, "The Evolving Internet," August, 2010, http://newsroom.cisco.com/dlls/2010/ekits/Evolving_Internet_GBN_Cisco_2010_Aug.pdf.

[19] John Perry Barlow, "A Declaration of the Independence of Cyberspace," 1996, https://projects.eff.org/~barlow/Declaration-Final.html.

[20] Lloyd's of London, "Business Blackout: the Insurance Implications of a Cyber-Attack on the US Power Grid," Emerging Risks Report 2015, May 2015, https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

[21] Council on Cybersecurity, "Critical Security Controls," 2014, http://www.counciloncybersecurity.org/critical-controls/.

[22] Comments provided in a private conversation in coordination with the report.

[23] Neal Pollard, in an email to Jason Healey.

[24] Richard Bejtlich, Statement for the Record for US House or Representatives Committee on Energy and Commerce, March 2015, http://docs.house.gov/meetings/IF/IF02/20150303/103079/HHRG-114-IF02-Wstate-BejtlichR-20150303.pdf.

[25] Barry Pavel and Peter Engelke, "Dynamic Stability: US Strategy for a World in Transition," Atlantic Council report, April 2015, http://www.atlanticcouncil.org/images/publications/DynamicStabilityStrategyPaper_04202015_WEB.pdf.

[26] Barry Pavel and Peter Engelke, "Dynamic Stability: US Strategy for a World in Transition," Atlantic Council report, April 2015, http://www.atlanticcouncil.org/images/publications/DynamicStabilityStrategyPaper_04202015_WEB.pdf.

[27] Such as Stanford University's "Clean Slate Program," http://cleanslate.stanford.edu/.

[28] The E15 Initiative, "Digital Economy," http://e15initiative.org/themes/digital-economy/.

Disclaimer and cautionary statement

This publication has been prepared by Zurich Insurance Group Ltd and the opinions expressed therein are those of Zurich Insurance Group Ltd as of the date of writing and are subject to change without notice. This publication has been produced solely for informational purposes. The analysis contained and opinions expressed herein are based on numerous assumptions. Different assumptions could result in materially different conclusions. All information contained in this publication has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Group Ltd or any of its subsidiaries (the 'Group') as to their accuracy or completeness. Opinions expressed and analyses contained herein might differ from or be contrary to those expressed by other Group functions or contained in other documents of the Group, as a result of using different assumptions and/or criteria. This publication is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Persons requiring advice should consult an independent adviser. The Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this publication. Certain statements in this publication are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by other factors that could cause actual results, developments and plans and objectives to differ materially from those expressed or implied in the forward-looking statements. The subject matter of this publication is also not tied to any specific insurance product nor will it ensure coverage under any insurance policy. This publication may not be reproduced either in whole, or in part, without prior written permission of Zurich Insurance Group Ltd, Mythenquai 2, 8002 Zurich, Switzerland. Zurich Insurance Group Ltd expressly prohibits the distribution of this publication[by/to/by or to] third parties for any reason. Neither Zurich Insurance Group Ltd nor any of its subsidiaries accept liability for any loss arising from the use or distribution of this presentation. This publication is for distribution only under such circumstances as may be permitted by applicable law and regulations. This publication does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

Zurich Insurance Company Ltd
Mythenquai 2
8022 Zurich
Switzerland

173000821 (09/15) TCL

ZURICH®