Risk Nexus

Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures

Frequently Asked Questions

How does information and communication technology (ICT) benefit the global economy?

This project groups the benefits of ICT into three main components, starting with the **direct contributions to GDP** from the ICT sector itself (for example, from well-known major ICT companies like Apple, Microsoft, Intel, or Google). These contributions are estimated to have grown to over 9 percent of total business value added in OECD countries, before declining somewhat as the industry moves to developing countries; the sector's global growth as a share of GDP is probably behind us. The second component is the **indirect contribution of ICT investments** to enhanced production and productivity across the broader economy; it is estimated to contribute between 20 to 30 percent of economic growth. Last is the surplus benefit that consumers gain (**consumer surplus**) from either decreased prices of the technologies or from improved capacity and quality of the technology at the same price. This benefit is smaller than that of the contribution of ICT to the broader economy.

How do ICT security problems cost the global economy?

The economic costs from ICT fall into three primary categories. First, the **direct spending** on cybersecurity solutions (such as firewalls and threat intelligence) is rising steadily, approaching 0.1 percent of global GDP; this value varies by country. For example, in the United States, spending may be upwards of 0.35 percent of US GDP. Second is the **cost of adverse cyber events**, such as recovering from a data breach or the value of stolen intellectual property, which were estimated by the Center for Strategic and International Studies as 0.64 percent of GDP in the United States. The third set of costs are the **opportunity costs**: the unrealized economic benefits due to the foregone use of technologies in fear of adverse cyber events, as well as benefits not realized because nations have not fully embraced ICT for a variety of reasons, including political controls on it.

How did we assess the economic costs and benefits from ICT?

The economic modeling used in this report started with extensive research to find the best literature and data on the economic benefits of ICT and the costs of security problems. The Pardee Center then extended the International Futures (IFs) forecasting system, building the capacity to display, analyze, and forecast the future of cyber costs and benefits. See below for more information on IFs.

Why did the report choose gross domestic product (GDP) as the benchmark against which to measure benefits and costs?

Using GDP allowed a common metric to compare benefits and costs across economies and time. As a standard indicator of economic size and strength, GDP allowed the results of this model to be more easily comparable and understandable, even to non-economists. Also, because this report on cybersecurity is only the first report in a series of three, using GDP allows the results of the following reports to be directly comparable.

What is the difference between annual and cumulative benefits and costs? Why do they accumulate differently over time?

When comparing costs and benefits of ICT, we need to distinguish between comparing annual values and the accumulation of costs and benefits over time. Most costs resulting from ICT, including spending on security and the impacts of adverse events, are either annual operating costs or one-off expenses. Either way, the costs have limited carry-forward impacts. In modeling terms, they are flows, with the costs paid annually and accumulating over time as a simple sum.

In contrast, cyber benefits in the form of increases to capital stock and productivity carry forward across time like capital in a bank account, delivering compounding rewards years after the initial investment.

As a result, it is possible that annual value of ICT risk-related costs could exceed incremental annual benefits in any given year. However, the accumulation of benefits exhibiting compounding growth (like compound interest) will grow so large over time that they will almost inevitably outpace costs, which accumulate in simple annual summation. Only risks so large that they cause societies to dramatically reduce or eliminate the use of the technology—and therefore to erase cumulative benefits—would tilt the cumulative balance toward the negative side.

How was the modeling done? What is the IFs modeling system?

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 (see http://www.pardee.du.edu/ for details and the model itself). 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.

IFs has several features of importance to the analysis: The IFs model represents 186 countries in different stages of socio-economic development and adoption of ICT technologies. It contains a set of heavily integrated and quite rich models: demographic, economic, human development (education and health), physical (energy, agriculture, and infrastructure), and socio-political (governance and government finance). This project enhances that model, especially in terms of the relationship between ICT infrastructure and the economy. The system also contains an interface that facilitates display and analysis of historical data as well as of forecasts and the development of alternative scenarios. This project enhances the IFs interface with a new display or dashboard focused on the benefits and costs of cyber technology (available at http://www.ifs.du.edu/ifs/frm_CyberDashboard.aspx). The system is freely open for use by anyone who may wish to make other assumptions and explore other possible futures.

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 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. The model incorporates measures of ICT penetration or pervasiveness 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.

What is the Base Case scenario?

The modeling of the costs and benefits of connectivity began with a 'Base Case.' The Base Case in the IFs integrated modeling system portrays a reasonable dynamic evolution of current patterns and trends, painting a picture of where the world is headed if these general trends continue without interruptions from unforeseen and disruptive geopolitical, economic, or technological events. When doing scenario analysis, the Base Cases serves as a good starting point with which we can compare alternate future scenarios. It allows us to estimate the relative effects of major changes predicted in the alternate scenarios against a likely 'status quo' version of the future.

In our report, development of ICT in the Base Case is based on the International Telecommunication Union's (ITU) ICT Development Index, which suggests a convergence in the prevalence of ICT across economies of different income levels as connectivity becomes universal. This is the basis against which we compare our alternate cyber futures.

To consider alternate futures, why did we choose these two axes of uncertainty – the 'awesomeness' of the Internet and government-control vs non-state control?

These two axes seemed to best represent not just many of the opinions of experts interviewed for this, and related projects, but also to best encapsulate many similar ideas. For example, other reports that look at alternate cyber futures included uncertainties like the pace of future technology development, the rate of uptake by consumers, or the strength of cyber defenses. By choosing alternate futures of *Cyber Shangri-La* (on the high end) and *Clockwork Orange Internet* (on the low) we could include or at least imply many of these related ideas.

Likewise, with so many headlines about government surveillance or fights between Washington, DC and Silicon Valley (for example, over full encryption), the other axis was able to imply so much with a simplification down to the corner cases of governments being the dominant power (the *Leviathan Internet*) versus companies and other non-states (the *Independent Internet*).

The future is of course not likely to look like any one of these four futures, but the two axes do help us to conceive of how the future might look different from today, and steer towards those which are most beneficial.

Why do we consider government-controlled Internet as something negative in terms of benefits to GDP?

This is an assumption, and one which is certainly open to debate. Specific government actions are expected to include setting up barriers against outside actors seeking to disrupt those benefits for particular countries or groupings of countries, and highly regulating actions by organizations and individuals that internationally or domestically may seek private benefits at the expense of others through activities such cybercrime. It is highly likely that such barriers and regulations would slow the growth of benefits. Many countries will erect barriers ostensibly for security, but perhaps more to protect domestic industries.

Moreover, the involvement of governments and the creation of cyber borders sharply raises the probability that governments escalate the militarization of cyberspace and domestic cyber policy. Nations will find it far more difficult to cooperate on critical cross-border cyber issues because they are no longer seen as technology issues, but core national security concerns.

Government regulation may improve cybersecurity, but there is not a strong precedent for believing it will be effective. Often, and not just in cybersecurity, regulation has driven compliance-based paperwork that has little actual positive impact. Some nations, in some industries, may enact smart and balanced regulations, but the assumption for this study is that it will be an overall drag on security and innovation.

How reliable are the data, and what are the implications of for our forecasts?

The analysis included roughly 150 different ICT-related data series. However, the data were limited, especially with regard to the economic costs of adverse cybersecurity events, and there was little comprehensive data across countries and time.

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. Therefore, instead of the exact numbers, the general trends identified in this report will help drive the global debate on cybersecurity problems and solutions.

Why do the benefits and costs of ICT vary so much by region and income group? Why have high-income economies already reached the cost/benefit inversion point, but low- and medium-income economies haven't?

Most of the ICT productivity literature points to ICT being considerably more widely adopted and having more of an impact on growth in developed countries than in developing countries. The differences between developed countries and developing countries can also be explained in part by the countries' 'capacity to benefit' from ICTs, including human capital (educational attainment, manpower skills), market structure, legal and institutional frameworks, supportive industries, transportation and distribution networks, and so on. Higher penetration and use of ICTs in a country is therefore clearly, and not surprisingly, associated with greater impact of ICTs on the country's economic growth—but also with higher costs generated by adverse use of that technology.

What do we mean by ICT saturation?

ICT saturation refers to a situation where the market for existing ICT products is no longer generating new demand for the technologies. At this point, further growth can only be created through the development of new ICTs, product improvements, or extensions of markets.

The Base Case of the modeling represents the rather conservative view implicit in the ITU's current ICT index that, because ICT impact has been driven by mobile and broadband penetration, there soon will be a convergence in the prevalence of ICT across economies of different income levels as such connectivity becomes increasingly universal and a general saturation of use. Of course, this isn't the only possible future, as future developments such as higher speeds, cloud computing, or the Internet of Things (IoT) might very well postpone market saturation.

What are other key assumptions that might have a big impact on the analysis?

The most significant assumptions are the projections of ICT advance to 2030 (see the FAQ concerning saturation), the potential productivity benefits of any given state of the technology, and similarly the costs associated with any anticipated pattern of its advance. The scenarios make alternative assumptions about each of these.

For instance, to provide a framework for the assumptions on adverse event costs, the Pardee Center created detailed matrices concerning the probability and unit costs of different adverse cyber events, including hacking, cybercrime such as identity theft, espionage including intellectual property theft, and cyber warfare. Data collected over the course of the research informed these matrices, but they also necessarily include assumptions about how the various adverse event costs play out through the Base Case and different futures. Other assumptions shape representation of the advance of ICT and the extent of its beneficial impacts.

The IFs model and all of the data and model parameters are available online, so other researchers can make their own assumptions and alter our scenarios or build their own. The Pardee Center and Atlantic Council welcome such additional analysis.

For more information, please contact Cyber@AtlanticCouncil.org.