Global Commission on Internet Governance

One Internet

CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

One Internet

CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

Global Commission on **Internet Governance**

ourinternet.org

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

Contents

Preface

Internet governance is one of the most pressing global public policy issues of our time. Some estimates put the economic contribution of the Internet as high as $4.2 trillion* in 2016.[1] The Internet of Things (IoT) could result in upwards of $11.1 trillion in economic growth and efficiency gains by 2025.[2] And, the Internet is more than simply a system of wealth generation; it also acts as a platform for innovation, free expression, culture and access to ideas. Yet across multiple levels, the Internet's basic functionality and the rights of users are under strain.

The Global Commission on Internet Governance (GCIG) was launched in January 2014 by the Centre for International Governance Innovation (CIGI) and Chatham House in response to trends toward fragmentation of the Internet, with the aim of offering guidance on how to address new challenges as they emerge. The Commission focused its recommendations on a call for a new global social compact to promote a single, open and secure Internet for all. Carl Bildt, former prime minister and former foreign minister of Sweden, chaired the Commission, comprised of 29 notable persons representing a range of Internet governance stakeholders as well as geographic regions. The Commission also benefited from the valuable contributions and participation of Kathy Brown, Anne Carblanc, Eileen Donahoe and Andrew Wyckoff.

A global Research Advisory Network (RAN) supported the Commission, producing more than 50 research papers on topics including Internet fragmentation, human rights, interconnection and

* All figures are in US dollars unless otherwise noted.

access issues, cyber-security cooperation, trade and development, and other Internet governance research areas. This scholarship informed the deliberations of the Commission and the recommendations put forward in this report. The Commission's diverse expertise, coupled with the RAN's theoretically and empirically grounded research, has given the Commission a unique opportunity to meaningfully inform and advance Internet governance debates.

The work of the Commission and the drafting of the report was supported by a secretariat whose members included Deputy Chair Gordon Smith, Commission Co-directors Fen Osler Hampson and Patricia Lewis, Senior Special Adviser Bill Graham, Director of Research Laura DeNardis, CIGI Research Fellows Samantha Bradshaw and Eric Jardine, Commission Co-managers Brenda Woods and Hannah Bryce, and Carol Bonnett, CIGI's publisher. We also thank Oonagh Fitzgerald, director of CIGI's International Law Research Program and Aaron Shull, CIGI's chief of staff and general council, for their guidance on legal matters.

The Commission's work also greatly benefited from two extensive public-opinion surveys conducted by CIGI and the global polling firm Ipsos on different aspects of Internet trust and security. The surveys provided the Commission with public input from more than 23,000 users in 24 different countries and territories, on a range of issues from Internet governance, Internet access, human rights and cyber security. The work of the Commission was also greatly enhanced by the many contributions of the Organisation for Economic Co-operation and Development (OECD) and McKinsey & Company on the economic analysis in the report.

THE COMMISSION

Carl Bildt, Sweden
Chair of the Global Commission on Internet Governance

Gordon Smith, Canada
Deputy Chair of the Global Commission on Internet Governance

Fen Osler Hampson, Canada
Co-Director of the Global Commission on Internet Governance

Patricia Lewis, United Kingdom
Co-Director of the Global Commission on Internet Governance

Laura DeNardis, United States
Director of Research of the Global Commission on Internet Governance

Sultan Sooud Al Qassemi, United Arab Emirates
Dominic Barton, Canada
Pablo Bello, Chile
Pascal Cagni, France
Moez Chakchouk, Tunisia
Dae-Whan Chang, Republic of Korea
Michael Chertoff, United States
Dian Triansyah Djani, Indonesia
Anriette Esterhuysen, South Africa
Hartmut Glaser, Brazil
Dorothy Gordon, Ghana
Angel Gurría, OECD
Dame Wendy Hall, United Kingdom
Melissa Hathaway, United States
Mathias Müller von Blumencron, Germany
Beth Simone Noveck, United States
Joseph S. Nye Jr., United States
Sir David Omand, United Kingdom
Nii Quaynor, Ghana
Latha Reddy, India
Marietje Schaake, Netherlands
Tobby Simon, India
Michael Spence, United States
Paul Twomey, Australia
Pindar Wong, Hong Kong

The Essentials

The Future of the Internet Hangs in the Balance

The world is embracing a truly digital future. Upwards of one billion new users and 20 billion devices are forecast to be online within five years. However, for this future to deliver its promise of greater digital freedom, security, trustworthiness and accessibility for all, governance of the Internet across all its dimensions must be an obvious priority around the world.

In only a few decades, the Internet has grown to be a truly transformative phenomenon, with the capacity to touch nearly every aspect of life. The Internet now connects almost half of the world's population and connectivity rates continue to expand apace, empowering users for both good and ill.

The Internet is unquestionably the most powerful information system the world has yet seen, but the digital world is only just past its infancy. As the digital world evolves, the Internet is poised to be *the* superstructure underlying all other infrastructures.

The Internet has become such a part of our lives that we take it, and our access to it, for granted. Maintaining and preserving its open and accessible qualities — the very qualities that encourage creativity and connectivity — present a challenge. It is vital that the rules and safeguards of Internet governance keep up with the pace of digital innovation, particularly in the sphere of the IoT. At the same time, the process of governance must not inadvertently slow down the spread of the Internet's benefits, reduce creativity or inhibit its global reach.

The structure of the Internet inevitably transcends sovereign borders, thereby engaging a wide range

of actors in its development and management. The Internet challenges traditional hierarchies and cultural boundaries. Its governance must therefore be based on both formal mechanisms and evolving norms to capitalize on its tremendous power to provide economic opportunity and security, while also providing resilience and privacy for all Internet users.

To realize its full potential, the Internet of the future will need to be open, secure, trustworthy and accessible to all. Safeguarding these attributes requires international cooperation that engages governments, businesses, the technical community and civil society in a shared vision to protect the rights of users, establish norms for responsible public and private use, and ensure the kind of flexibility that will encourage innovation and growth.

Grounded in an extensive program of research, individual consultations, public opinion surveys and enriched by our Commissioners' wide experience, diverse geographical backgrounds, and gender and stakeholder representation, this report lays out a comprehensive approach for realizing a future with digital freedom, security, trustworthiness and accessibility for all. It outlines the rights and responsibilities of all actors, each playing a critical role in shaping the future of the Internet.

Three Possible Futures of the Internet

The Internet as we know it in 2016 will not be the Internet of the future. The following scenarios explore a range of possibilities from a possible worst case to an ideal case. These are not the only possible scenarios, of course, and they have been put in stark relief for emphasis. They convey the possible courses of development the Internet-enabled world now faces. Citizens can shape the evolution of the digital world, but that process begins with actively choosing what sort of future we want for the Internet and, ultimately, how everyone will be impacted by the Internet. The time for that decision is now, and everyone needs to be involved in making the decision.

To realize its full potential, the Internet of the future will need to be open, secure, trustworthy and accessible to all.

A Dangerous and Broken Cyberspace

The worst-case scenario is one in which the Internet breaks on our watch. In this scenario, the costs imposed through the malicious actions of criminals and inadvertent effects of government regulation of the Internet are so high that individuals and companies curtail their usage. Governments impose sovereign-driven restrictions that further fragment the Internet and violate basic human rights. The proliferation of the IoT into all aspects of daily life is accompanied by unprecedented private data collection and government surveillance, which destroy users' privacy and present terrifying new opportunities for widespread criminal breaches in cyber security and even the possibility of cyberwarfare, including attacks on civilian infrastructure such as the power grid or water systems.

The cost of cybercrime in 2016 may be as high as $445 billion. That figure could grow as high as two trillion dollars a year in 2019 and continue to increase to as much as three trillion dollars annually by 2020. In this worst-case scenario, newly connected users become easy targets for commercial exploitation, fraud and cybercrime. Increasingly, proprietary data and personal information are illegally copied and reused; online and other critical services are disrupted electronically; systems are erased or destroyed; and sophisticated malicious actors — including state agencies — often remain undetected despite being very active. Invasive privacy violations and online abuse, whether as a result of massive corporate data collection or unrestrained government or private surveillance, discourage Internet use. The public becomes increasingly concerned about the secretive

ways that algorithms are used to collect data on their preferences, and by whom. In such a world, people simply stop using the network and its potential is lost.

Uneven and Unequal Gains

The second scenario is one of stunted growth, where some users capture a disproportionate share of "digital dividends" while others are permanently locked out. Governments do not preserve the Internet's openness, enable competition and encourage the private sector to expand high-speed access, leaving more than three billion people off-line. A world of digital haves and have-nots results, increasing inequality and unrest across the board. The economic value of the Internet is compromised by governments failing to respond appropriately to the challenges of the digital era, choosing instead to assert sovereign control through trade barriers, data localization and censorship and by adopting other techniques that fragment the network in ways that limit the free flow of goods, services, capital and data. The costs of this more optimistic scenario could be immense.

The splintering of the network could lead to reductions in national GDP of greater than one percent per year, a reduction in domestic investment of more than four percent, an almost two percent reduction in exports and aggregate welfare losses ranging into the hundreds of billions of dollars. A fragmented Internet would also impinge upon people's right to free expression, privacy and access to knowledge. Walled gardens and overly restrictive intellectual property regimes limit knowledge sharing, stifling innovation. Industry's adoption of proprietary, anti-competitive business practices that do not respect individuals' choices over how their data is used exacerbate these concerns. While the world will muddle along in this scenario, a great deal will be lost and many will be unjustly left behind.

Broad, Unprecedented Progress

In the third scenario, the Internet is energetic, vigorous and healthy. A healthy Internet produces unprecedented opportunities for social justice, human rights, access to information and knowledge, growth, development and innovation. The Internet revolution of the past two decades has already changed the nature of communication and commerce for more than three billion global users, and its economic impacts and productivity benefits continue to spread far beyond the estimated $6.3 trillion — or eight percent of global GDP — that the Internet contributed in 2014. The expansion of both fixed and mobile broadband penetration brings billions of new users online, narrowing digital, physical, economic and educational divides. The IoT, now pervasive, leads to the secure interconnection of devices, plausibly resulting in GDP growth of up to $11.1 trillion by 2025.

The creation of interconnected smart cities improves the quality of life for much of the world's population, while helping to reduce carbon emissions. Global societies and economies begin to realize the opportunities for transformation made possible by the adoption of new Internet-enabled technologies such as driverless cars, distributed digital ledgers and three-dimensional (3D) printing. Internet-supported distributed energy production and consumption networks deliver greater energy efficiency and support widespread conversion to renewable energy. The use of distributed ledger and blockchain technologies provides globally circulated, trusted records and transfers of value to deliver a wide range of services. Economies with aging populations find new sources of productivity, as the elderly live better lives and enjoy greater health. Government and industry act collaboratively across borders to manage the risks of online activity. This is the scenario to which most of the world aspires, but technology alone will not be able to achieve it. Realizing this future requires concrete actions to ensure that the Internet will be open, secure, trustworthy and inclusive of everyone.

The Future of the Internet Depends upon a New Social Compact

The Commission envisions a world in which the Internet reaches its full economic and social potential, where fundamental human rights such as privacy and freedom of expression are protected online. This optimistic future can only be achieved if there

CORE ELEMENTS OF A SOCIAL COMPACT FOR THE DIGITAL SOCIETY

There must be a mutual understanding between citizens and their state that the state takes responsibility to keep its citizens safe and secure under the law while, in turn, citizens agree to empower the authorities to carry out that mission, under a clear, accessible legal framework that includes sufficient safeguards and checks and balances against abuses. Business must be assured that the state respects the confidentiality of its data and they must, in turn, provide their customers the assurance that their data is not misused. There is an urgent need to achieve consensus on a social compact for the digital age in all countries. Just how urgent is shown by current levels of concern over allegations of intrusive state-sponsored activities ranging from weakening of encryption to large-scale criminal activity to digital surveillance to misuse of personal data, and even to damaging cyber attacks and disruption.[3]

is universal agreement to collectively develop a new social compact ensuring that the Internet continues on track to become more accessible, inclusive, secure and trustworthy.

An Open Internet

The network needs to remain open, allowing data to flow freely based upon the architectural principle of efficiency and non-discrimination, as well as the normative principle of freedom of expression. Protocols and platforms should be open to all, allowing for spontaneous innovation based on the infrastructure of the network. These vital components of the Internet should be protected, and not manipulated to achieve some local or short-term regulatory purpose.

Free expression is a fundamental human right and the foundation for innovation (both economic and political) to take place. Governments must resist initiatives that are harmful to the basic rights of people and detract from the innovative potential of the Internet.

For unhindered innovation to take place, it is vital that the Internet's logical layer remains interoperable based on standards that are openly developed and available.

An open Internet is increasingly central to the global economy and the unrestricted flow of goods, services, capital, data and skills. Government or commercial efforts to take advantage of the Internet for short-term political or economic gains must be recognized as counterproductive over the long term, and therefore avoided.

The only certainty in a digital world is constant change. Adaptability and resilience are key. Civil society, the technical community, the private sector and governments have shown themselves to be adaptable and capable of dealing with unanticipated opportunities and challenges. When the voices of all stakeholders are heard in the policy process, more sustainable outcomes are achieved. All stakeholders need to respect and participate in this system of governance in support of the open, universal and resilient Internet.

A Secure Internet

Security cannot be treated as an afterthought, trailing technological innovation, nor is it an issue for governments alone. Personal freedom, economic growth and innovation, particularly in the IoT, will be degraded if the digital space is not sufficiently secure and all actors do not practise better digital "hygiene." The world could be left with an "Internet of Threats" rather than an "Internet of Trust" if systems are not designed and deployed with security and resilience at their core.

Governments should not create or require third parties to build back doors or compromise encryption standards, as these efforts would weaken the Internet and fundamentally undermine trust. Efforts by the technical community to incorporate privacy-and-security-enhancing solutions into all standards and protocols of the Internet should be encouraged.

The Commission urges member states of the United Nations to agree not to use cyber technology to attack the core infrastructure of the Internet. Governments seeking a peaceful and sustainable Internet should adopt and respect norms that help to reduce the incentive for states to use cyber weapons. Governments should agree on infrastructure assets and services that must not be targeted by cyber attacks.

Businesses or other organizations that transmit and store personal data using the Internet must assume greater responsibility to safeguard that data from illegal intrusion, damage or destruction. Institutions should demonstrate accountability and provide compensation in the case of a security breach.

Manufacturers and vendors of information and communication technologies (ICT) should follow the principle of privacy and security by design, when developing new products, paying particular attention to embedding security in the burgeoning IoT. They must be prepared to accept legal liability for the quality of the technology they produce. Buyers of ICT products should also collectively demand that manufacturers respond effectively to concerns about privacy and security. Governments can play a positive role by incorporating minimum security standards in their procurement processes.

Businesses should purchase cyber insurance to cover the liability costs of breaches of their systems. Cyber liability insurance vendors can be persuasive in promoting best practices in the corporate sector. Cyber premiums should be higher if best practices are not followed. Insurers need to have better data to appropriately identify and price cyber risk and to develop appropriate products. Government regulations should require routine, transparent reporting of technological problems to provide the data required for a transparent market-based cyber-insurance industry.

A Trustworthy Internet

For the Internet to reach its full potential, governments, companies and other users need to act in ways that preserve the trustworthiness of the network. In the absence of trust, users will modify their behaviour by curtailing their online activities or by turning to closed proprietary solutions that, in turn, alter the fundamental end-to-end principle of online engagement that has made the Internet a robust platform for growth, development and innovation. These challenges, already large, will be exacerbated by the growth of the IoT.

There is a need to reverse the erosion of trust in the Internet brought about by indiscriminate and non-transparent private practices such as the collection, integration and analysis of vast amounts of private information about individuals, companies and organizations. Private surveillance based on “big data” is often conducted under the guise of a free service. Individual users of paid or so-called free services provided on the Internet should understand, and have some choice over, the full extent of the ways in which their data will be used and exploited for commercial purposes. Users should not be excluded from the use of software or services that allow them to participate in the information age, and they should be offered the option of purchasing a service without having to agree to give the provider access to their personal information. International rules are also required to ensure that the holders of large repositories of data are transparent about how they collect, use and share user-generated data.

Interception of communications, collection, analysis and use of data over the Internet by law enforcement and government intelligence agencies should be for purposes that are openly specified in advance, authorized by law (including international human rights law) and consistent with the principles of necessity and proportionality. Purposes such as gaining political advantage or exercising repression are not legitimate.

The emergence of technologies such as distributed ledger technologies enable people who have no direct knowledge or assurance in each other to collaborate

without having to go through a traditional central authority. This technology enables established businesses and entrepreneurs to devise new platforms for the secure and transparent exchange of value — indeed, anything that can be reflected in an agreement. But the introduction of such technologies will have profound impacts on traditional governmental and private institutions that supply dispute and arbitration services to communities. Understanding and preparing for these impacts is essential, especially in those developing economies where such institutions are already weak.

An Inclusive Internet

The Internet has connected more than three billion people in just a few decades, however, over half of the world's population remains off-line. If the rest of humanity is not given the opportunity to come online, digital and physical divides both within and between societies will widen, locking some into a permanent cycle of exclusion from an increasingly digital global economy.

Countries cannot hope to compete in the global marketplace of ideas if their business communities and broader populations are not online. To guarantee access, governments need to encourage the continuing improvement of Internet infrastructure, ranging from Internet exchange points (IXPs) to terrestrial and space-based systems, undersea cables and emerging access technologies. Most importantly, governments should use competition as a tool to expand Internet access facilities to the maximum extent possible, while investing to ensure availability when market forces prove insufficient. In addition, public investment at locations such as schools and libraries can also be leveraged to provide wider access to communities that would otherwise have limited opportunities due to factors such as income or geography. In many places, skills and education are critical barriers preventing people from using the Internet to its full potential. Governments have an opportunity to incorporate digital literacy into schools so that everyone can learn to fully engage in the digital world. Additionally, actions can be taken to increase demand through encouraging the development of locally relevant content and services, as well as the necessary skills to use ICTs and the Internet.

The expanded use of the Internet is having a significant effect on the nature of work and the structure of industries.

The expanded use of the Internet is having a significant effect on the nature of work and the structure of industries. The disruption to traditional jobs and skill requirements can create economic hardship and civil discontent. Rather than attempting to preserve old jobs by stifling innovation, governments should help workers adapt to the new economic reality via skills training and educational programs.

For people with disabilities, accessing the benefits of the Internet often requires more than simply an interconnected device. Governments have an obligation to create incentives for the development and adoption of Web standards that ensure that everyone, regardless of their physical capacities, can use the Internet.

What Happens Next?

The Internet has indeed reached a crossroads. Choices need to be made — and making no choice is itself a choice. It is all about who should have what power to control the future of the Internet. The Internet has fundamentally altered the world, and as the next billion and the next after that join the global conversation the Internet has enabled, it will continue to transform the world. The changes we will see can be fundamentally beneficial, or destructive, perhaps even rolling back the gains that have been made. It is up to us as individuals, as members of civil societies, in our roles in business, in governments and in our

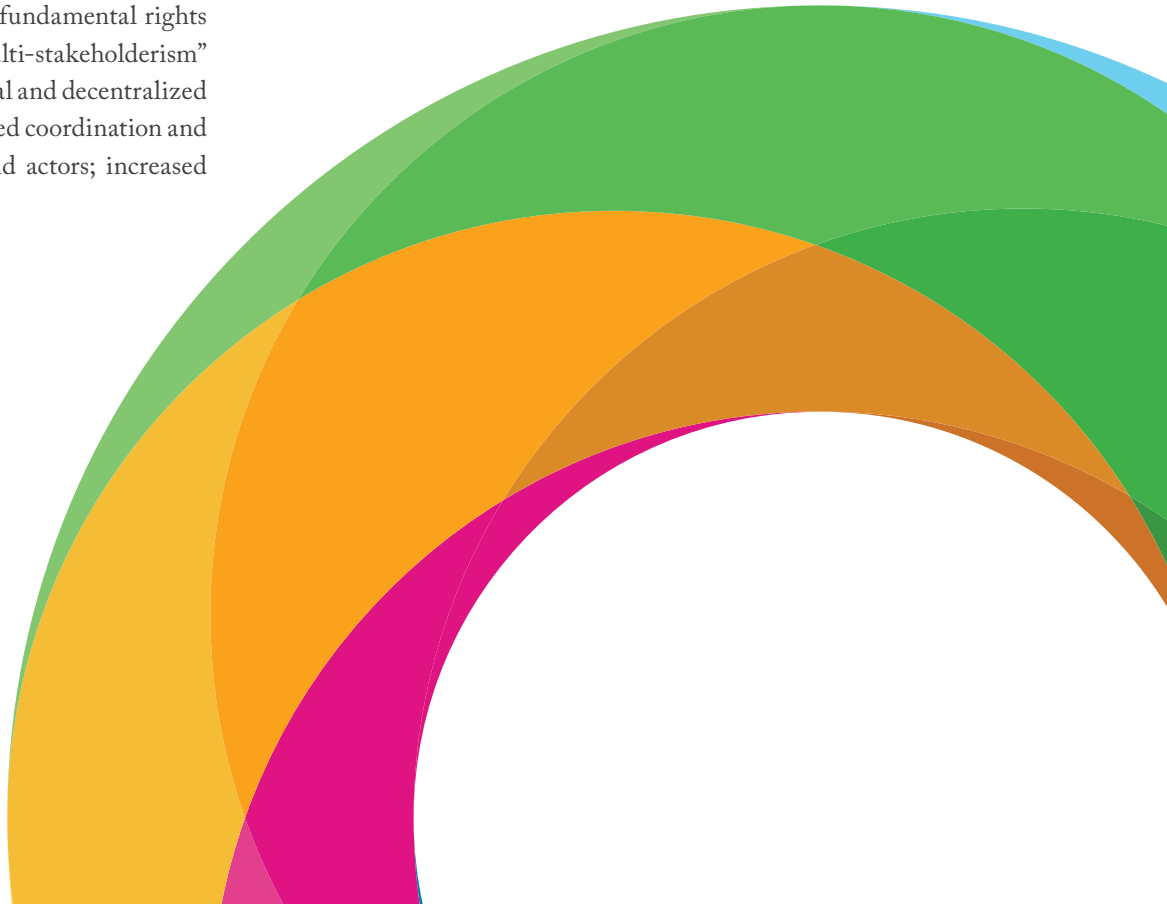
communities, to determine which direction the transformation will take. In writing this report, the GCIG is, we believe, providing practical advice on the steps everyone needs to take to achieve a positive, creative outcome.

Our advice is based on the belief that only a normative approach can address the myriad challenges facing Internet governance. We call on governments, private corporations, civil society, the technical community and individuals together to create a new social compact for the digital age. This social compact will require a very high level of agreement among governments, private corporations, civil society, the technical community and individuals. Governments can provide leadership, but cannot alone define the content of the social compact. Achieving agreement and acceptance will require the engagement of all stakeholders in the Internet ecosystem.

Success in this endeavour requires collaboration to refresh and extend the model of a multi-stakeholder process that has thus far empowered the growth of the Internet, and to conceive of a new model that embraces greater involvement of those whose lives are affected by decisions that govern their ability to use the network and to exercise their fundamental rights online. This new vision of "multi-stakeholderism" requires a more collaborative, global and decentralized model of decision making; enhanced coordination and cooperation across institutions and actors; increased interoperability in terms of identifying and describing issues and approaches for resolution throughout the ecosystem; open information sharing and evidence-based decision making; and expertise- or issue-based organization to allow for both localization and scale in problem solving.

Internet innovation will bring billions of new users online, creating new opportunities, and benefits as well as new threats. The present understanding of who needs to be involved in Internet governance must expand and evolve to accommodate new interests and newly concerned parties. To continue to be effective, Internet governance will need to be more inclusive and more distributed.

We believe it is possible to achieve all of this before the many worst-case scenarios posited for the future of the Internet occur. But we also believe that achieving this vision is only possible if all stakeholders commit to making this new model a reality, through an iterative consensus-building approach to creating a new Social Compact for the Digital Society. From our diverse geographic and stakeholder backgrounds, we are committed to achieving success, and invite you to join in the process.



Introduction

The Commission presents this report with the aim of providing high-level strategic advice and recommendations to policy makers, private industry, the technical community and other stakeholders interested in maintaining a healthy Internet. Just as every stakeholder has a legitimate role to play in Internet governance, so too do they have a responsibility to act in a way that promotes the freedom, openness and security of the Internet. Failure to maintain a healthy Internet will undermine opportunities for economic growth, free expression, political equality and social justice.

The Commission framed its work with reference to the working definition of Internet governance, developed by the United Nations World Summit on the Information Society (WSIS) in the Tunis Agenda: "A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[4]

This definition highlights several important concepts — first, that all segments of society play a role in Internet governance in their areas of expertise or authority. Second, it emphasizes that principles, norms, rules and decision-making procedures must be shared. And third, that Internet governance is concerned not only with the Internet's design and administration, but also with its evolution and use, so Internet governance is inherently oriented toward the future and the impact on society.

Implicit in the definition is the recognition that a large number of diverse tasks are undertaken by various stakeholders. These include developing public policies on issues such as privacy, intellectual property rights enforcement, access and interconnection, as well as technical governance functions such as protocol design

and the administration of Internet names and numbers. Actors across the Internet governance ecosystem have reached a number of high-profile influential agreements. Positive developments have followed the NETmundial meeting in Brazil, and the decision to transition the oversight of the Internet Assigned Numbers Authority (IANA) functions from the US government to a multi-stakeholder body, to name a few.

Despite these and other advances, global Internet governance is at a critical juncture. The Commission was formed in response to a number of tensions, both between states and among all combinations of states, private corporations, the technical community and civil society.

A partial list of the trigger points for these tensions includes the following:

- Terrorist attacks around the globe in recent years have prompted many governments to extend access to digital communications by police and intelligence services. As well as alarming citizens, this has led to contention between governments and private companies that want to provide encryption by default on their devices and services, while other companies are resisting domestic law enforcement efforts to gain access to data held in company servers abroad.
- In 2012, the World Conference on International Telecommunications (WCIT) meeting led to significant disagreement among states about governance matters, including how carriers are compensated for the exchange of data between networks. Some countries wanted (and still want) a larger role for governments in Internet governance (particularly with respect to the exchange of traffic between networks), while many others endeavoured to maintain the current multi-stakeholder model of Internet governance, where governments, private sector actors, the technical community and civil society all have a legitimate role to play.
- While a positive development, the 2014 announcement by the US government of a transition of the oversight of IANA functions from the Department of Commerce to a multi-stakeholder body created some stress in the Internet governance arena due to uncertainty over both timing and the ultimate implementation of the community's final proposal for a new model.
- There is a growing concern about the market power and data collection capabilities and practices of the large Internet platform companies as well as other private data intermediaries. The announcement of investigations into some companies is a regulatory response significantly driven by consumer concerns.
- The emergence of distributed ledger technologies has the potential to disrupt the business models of banks and the governance mechanisms of other institutions.
- The failure to incorporate security as an essential design feature by vendors and larger customers of the IoT raises concerns that its explosive growth could result in the "weaponization of everything." The drive to reap the private economic benefits of the IoT, serving a very diverse range of industries and capabilities, runs in tension to the public good of ensuring security and the certainty of data ownership.

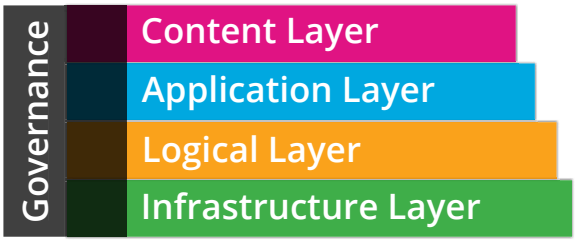
Responding to these and other increasing strains in this report, the GCIG speaks to the ways Internet governance can evolve to better secure the current and future potential of the Internet. The report intentionally provides concrete recommendations and points to actions that should be undertaken by various actors to help secure our collective digital future. As you would expect from such a diverse group of Commissioners, not everyone agrees completely with every detail of these recommendations; however, every Commissioner supports the report as a whole.

The sections each address a specific topic, but the Commission recognizes that some themes are so foundational to Internet governance that they need to be highlighted throughout the entire report. For example, governance questions regarding human rights, development, fragmentation of the Internet and trust all cross-cut specific issues such as trade, accessibility, security and privacy. These themes thus permeate the entire report.

What Do We Mean When We Say "The Internet"?

The Internet is not one homogeneous system, but an ecosystem of technologies, protocols, hardware, software and content. Because of this complexity, it can be helpful to think about the Internet in layers. There are many possible taxonomies for these layers, but one simple framework that makes sense in the context of this report disaggregates components of the Internet into four layers: infrastructure; logical; application; and content. It is the assumption of the Commission that there is no separate policy layer because policy questions permeate all of the various layers. Governance and coordination across layers are carried out by a combination of private sector policies, new global institutions, national laws and international cooperation.

Figure 1: The Different Layers of Internet's Structure



Source: Authors.

The infrastructure layer includes routers, switches, IXPs, transmission facilities such as fibre optic cable, cellular systems, IoT structures and systems, and various types of other hardware. The majority of this infrastructure is owned and operated by the private sector and, especially, telecommunications systems. Among the many policy issues at this layer are the questions of how to secure infrastructure, provide interconnection among telecommunication providers, enable interoperability among IoT infrastructure and bring affordable broadband access to communities.

The logical layer of the Internet includes Internet-unique virtual resources and technical standards. Examples of software-defined critical Internet resources include Internet Protocol (IP) addresses and domain names, as well as the domain name system (DNS), the distributed system that translates between the domain names that people use and the binary IP addresses that computers use to route information. A complex system of institutions allocates and assigns these resources and operates the underlying system, and questions about the oversight of this area has been a long-standing policy issue in Internet governance. The logical layer also includes Internet standards, the Internet's common language establishing protocols for how information can be interoperable and exchanged among devices, regardless of the manufacturer. Prior to the development of the Internet's core protocols, such as TCP/IP (which stands for Transmission Control Protocol/Internet Protocol), devices made by one company could not exchange information with another company's equipment. The development of the World Wide Web core protocols and standards, such as Hypertext Transfer Protocol and Hypertext Markup Language, enabled information exchange across different software and hardware platforms. The open and interoperable protocols underlying Internet technologies and applications are established by institutions such as the Internet Engineering Task Force (IETF), which sets most of the core Internet protocols, and the World Wide Web Consortium (W3C), which sets standards for the Web. The openly available standards established by these institutions were the revolutionary building blocks that enabled not only the possibility of worldwide Internet connectivity, but also the rapid innovation environment in which anyone could develop new products based on these standards.

The application layer of the Internet includes the software with which end users and IoT devices directly interact. The most prominent application on the Internet is the World Wide Web. Although the Internet predated the World Wide Web by decades, it was the Web that enabled the easy usability, commercialization and globalization of the Internet. Among the many other applications that use the Internet are mobile apps, voice over IP applications, search engines, social media platforms and platforms for sharing user-generated content. The range of possibilities afforded by Internet technologies, design choices and policy environments within these applications have significant public interest implications in areas as diverse as individual privacy, free speech, intellectual property rights enforcement and protection of the vulnerable.

The content layer of the Internet is the one most visible to end users. Internet content obviously includes alphanumeric text (messaging, IoT data, email, web content and books), audio (music and voice calls), pictures (photographs, diagrams, digitized art and illustrations), video (user-generated video, video conferencing and streaming movies) and multimedia of all kinds (video games, virtual reality, IoT environments). Policy issues around content are numerous, including censorship, intellectual property rights and access to knowledge.

Throughout this report, when we refer to the Internet we include the Web and applications that provide access to content. When a distinction needs to be drawn among these, that will be indicated.

A Fine Balance: Promoting A Safe, Open and Secure Internet

The Internet Has Generated Tremendous Wealth, Innovation and Opportunity

The Internet is revolutionizing how humans work, play and live. From its early beginnings in research laboratories, the Internet has expanded into a system with a global reach and global ramifications. Five years ago, the McKinsey Global Institute (MGI) found that Internet-related consumption and expenditure had already surpassed the size of the global agriculture and energy sectors. More recently, MGI has estimated that the Internet contributed some $6.3 trillion, or eight percent of global GDP, in both direct value and productivity gains as of 2014. The impact is continuing to grow rapidly, albeit unevenly across sectors and countries.

A number of disruptive Internet-enabled technologies currently on the horizon or in the early stages of adoption — including autonomous vehicles, 3D printing and next-generation genomics — are likely to accelerate this momentum in the very near future. In particular, the IoT alone could create some $11 trillion in economic value by 2025, as the physical world becomes more networked.[†] One study has estimated that the IoT could yield some $4.6 trillion dollars solely in public-sector efficiency gains.[5]

[†] Projections based on technology studies from the MGI, including "Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity" (2011); "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy: (2013); and "The Internet of Things: Mapping the Value Beyond the Hype" (2015). Note that the estimate of the Internet's 2014 economic impact was derived by combining measurement of digital capital and econometric frontier analysis; it encompasses both direct impact and productivity effects.

Figure 2: The Far-reaching Potential of the IoT

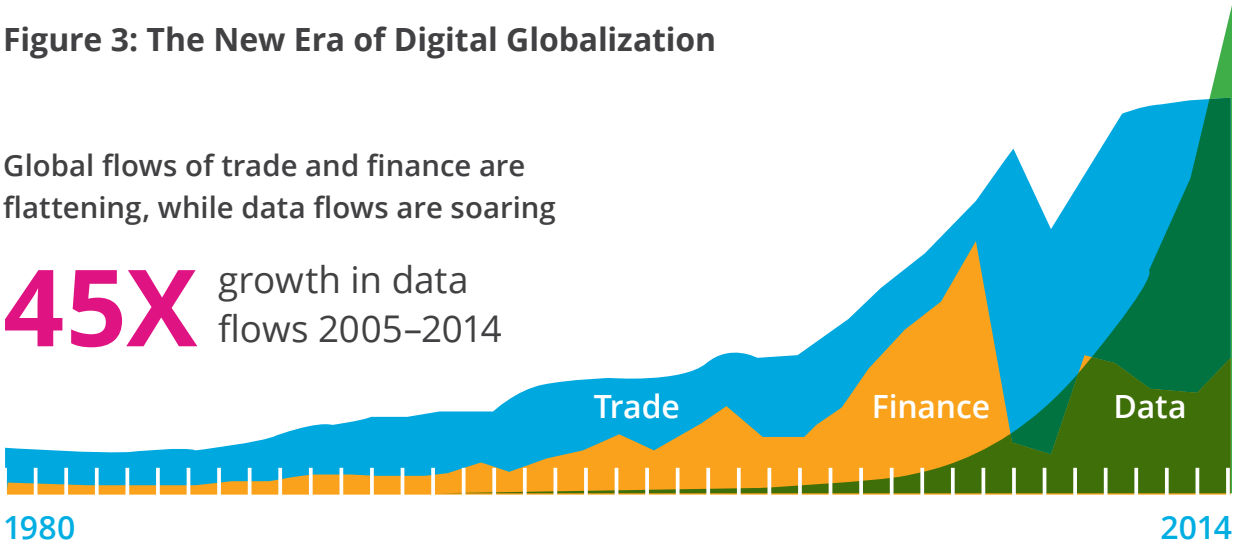
Source: McKinsey Global Institute, 2015.[6]

Furthermore, estimates suggest that cross-border data traffic has increased by a factor of 45 times in the past decade and is projected to increase by an additional nine times over the next five years. Companies increasingly rely on the Internet to interact with their foreign operations, suppliers and customers — and to access the best talent, inputs and ideas from around the globe. Cross-border data flows contributed some $2.8 trillion to global GDP in 2014, surpassing the value of global trade in goods and changing the way business is conducted across borders.[7]

The benefits of the Internet are not strictly economic. As indicated by the 2014 CIGI-Ipsos Global Survey on Internet Security and Trust, the Internet has also given billions of users around the world a tool for free expression, social and political engagement, and access to knowledge, as shown in Figure 4.

The Internet has given us the greatest access to information the world has ever seen. Free expression, innovation and access to new ideas have flourished. Societies have been changed by the Internet's capacities: lower costs of communication have enabled the creation of new types of virtual, interest-based communities across the breadth of human activities; individuals have been empowered by a previously unthinkable access to information and knowledge; support networks have grown to span the globe, including those providing support for migrants and refugees; new patterns of work, collaboration and leisure-time activities have increasingly become the norm; and national and global political environments

Figure 3: The New Era of Digital Globalization

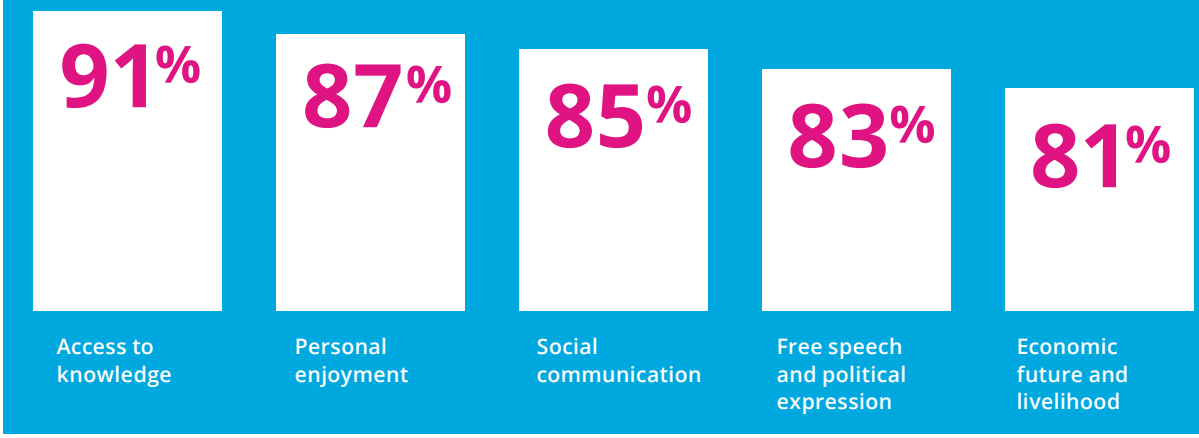


Source: McKinsey Global Institute. Used with permission.

have been very much altered, whether in terms of engagement in conventional party politics or the development of strong lobbying and issue-based movements, such as the world-wide campaign against global warming.

In the world of commerce, the Internet has also brought opportunities for economic growth. International trade has been facilitated not just for existing businesses, but also for new enterprises small and large, as they connect remotely with suppliers and customers. The phenomenon of global value chains has been turbocharged by Internet openness. Firms in developed and emerging economies are now able to enter into supply chains and open up new markets for products and services. We see collaborative research on a global scale, with publications, patents, researchers, and academic and research institutions taking on international dimensions and drawing on cross-border knowledge flows to address global challenges such as climate change and infectious diseases. Market entrants bubble up with new

Figure 4: The Benefits of the Internet



Source: CIGI-Ipsos Global Survey, 2014. Available at www.cigionline.org/internet-survey.

innovative ideas, and firms can design, develop and deliver their products and services worldwide thanks to Internet-based crowd financing, digital utilities, professional services, micro-manufacturing, innovation marketplaces and e-commerce platforms. In the next few years, the Internet will become *the* infrastructure underlying all other infrastructures. All of this has been achieved with an underlying political, technological and economic governance model that has developed in an organic manner, without the benefit of a global "master plan." That model had its beginnings among the scientists and engineers who pioneered multi-stakeholder policy making in the technical design of the Internet.

Internet Governance: A Complex and Distributed Landscape

The Internet originated in the search for a set of engineering rules that would allow different kinds of computers to communicate with one another, even though they used incompatible network operating systems. To be fair, those who developed the Internet did not think of their work as governance at all. Steven Crocker, who developed the Request for Comments (RFC) series, which codifies the IETF's engineering rules and standards, described their situation this way: "Most of us were graduate students and we expected that a professional crew would show up eventually to take over the problems we were dealing with…"[8] That has yet to happen, but the benefits of having a simple way to communicate among different computers was soon recognized widely, leading to a rapid expansion of the Internet well beyond the world of research.

The success and rapid spread of the Internet arose from the fact it is simply a network of interoperating networks. Most of those are privately owned, yet the Internet is not controlled by any one of those networks in a way that promotes its own exclusive self-interest. As Andrew Sullivan, chair of the Internet Architecture Board, recently wrote: "The Internet is a radically distributed system: almost all of the technical operation is undertaken without any direct co-ordination with anyone, performed by an enormous number of independent operators. This means that interoperation is fundamentally a voluntary thing (aside from a minimal amount of central coordination; for example, of addressing systems and common protocols). In your network, you make your rules, and there is no stick (outside of national law) to make you interoperate with others. Instead, there is only the carrot: if you interoperate, you get the benefits of that interoperation."[9]

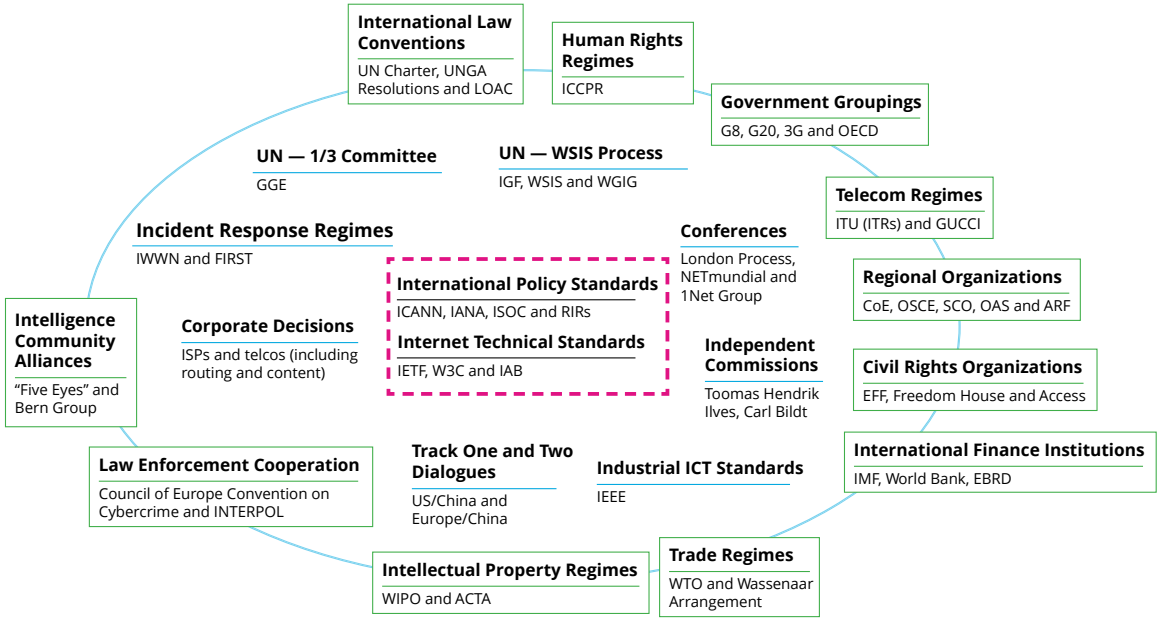
While this is true at the level of basic interconnection, as increasingly sophisticated and built-for-purpose applications are deployed on the Internet, it becomes obvious that rules made locally can have global effects. Rules made to increase the efficiency or convenience of one network or application now can have wide and unforeseen impacts on others, and this has made the engagement of all affected stakeholders a matter of increasing importance. Nonetheless, the coordination is still voluntary in nature, and a complicated mix of open and closed (proprietary or commercial) protocols maintains the balance in the system. It was the openness of the standards and protocols bequeathed to us by the Internet pioneers that enabled the amazing innovation we saw in the Internet's early years. As applications became more widely used, commercial interests flourished and unforeseen issues arose that affect everyone, such as security, privacy and trust, and an increasing drive toward developing closed, proprietary solutions. Thus, maintaining a balance to enable innovation and universal accessibility while increasing the confidence and trust of end users in a secure and resilient Internet remains a challenge today, especially as we look toward a future that includes the IoT.

As a result, today's Internet governance landscape is complex and challenging to those who wish to participate. It encompasses debates in the technical, economic, political, social, military, law enforcement and intelligence spheres, and those debates take place in forums that are by turns national, regional and international. If that was not complex enough, there is broad recognition that if it is to be effective and accepted as legitimate, Internet governance should be multi-stakeholder, involving and taking into account the views and needs of governments, the private sector, civil society and technical actors.[10] The term "multi-stakeholder" is

overused in the realm of Internet governance, but if used accurately, it can tell us a great deal. The term is used here to mean a model in which affected stakeholders who want to participate in decision making can, yet where no single interest can unilaterally capture control.

Internet governance should be understood as being embedded in a broader set of rules, institutions and processes that govern the management of cyberspace, covering related issue areas including trade, development, security, law enforcement and intellectual

Figure 5: The Regime Complex for Managing Global Cyber Activities



Acronyms for Figure 5

ACTA	Anti-Counterfeiting Trade Agreement	GUCCI	Global Undersea Communications Cable Infrastructure	IWWN	International Watch and Warning Network
ARF	Association of Southeast Asian Nations Regional Forum	IAB	Internet Architecture Board	OAS	Organization of American States
CoE	Council of Europe	IANA	Internet Assigned Numbers Authority	OECD	Organisation for Economic Co-operation and Development
DAC	Development Assistance Committee (OECD)	ICCPR	International Covenant on Civil and Political Rights	OSCE	Organization for Security and Co-operation in Europe
EBRD	European Bank for Reconstruction and Development	ICT	information and communications technology	RIRs	regional Internet registries
EFF	Electronic Frontier Foundation	ICT4D	Information and Communication Technologies for Development	SCO	Shanghai Cooperation Organisation
FIRST	Forum for Incident Response and Security Teams	IEEE	Institute of Electrical and Electronics Engineers	telcos	telecommunications company
"Five Eyes"	Alliance of Australia, Canada, New Zealand, the United Kingdom and the United States	IETF	Internet Engineering Task Force	UNGA	United Nations General Assembly
G8	Group of Eight	IGF	Internet Governance Forum	W3C	World Wide Web Consortium
G20	Group of Twenty	IMF	International Monetary Fund	WSIS	World Summit on the Information Society
GGE	Group of Governmental Experts (UN)	ISOC	Internet Society		
		ITRs	International Telecommunication Regulations		

Source: Joseph S. Nye, Jr., 2014. [12]

property, among others, in what is known as a regime complex.[11] This regime complex is not an integrated institution with the authority to impose regulation through hierarchical rules; however, neither is it merely an collection of highly fragmented practices and institutions with no identifiable core and non-existent linkages.

The oval map of cyber governance activities shown in Figure 5 attempts to help visualize this situation. The map mixes norms, institutions and procedures, some of which are large in scale, while others are relatively small; some are quite formal and some very informal. The labels are often arbitrary, and it is deliberately incomplete. Yet, it is a useful corrective to the usual United Nations versus multi-stakeholder dichotomy as an approach to cyber governance, and it locates Internet governance within the larger context of cyber governance. This map indicates the extent and wide range of actors and activities related to governance that exist in the space. Second, it separates issues related to the technical function of connectivity, such as the DNS and technical standards where a relatively coherent and hierarchical regime exists, from the much broader range of issues that constitute the larger regime complex. Third, it encourages us to think of layers and domains of cyber governance that deal with large, crosscutting issues such as security, human rights or development. And finally, it suggests that Internet governance now often includes actors whose primary responsibilities only tangentially include Internet issues. As noted earlier, these actors are often tempted to try to accomplish objectives relating to patterns of Internet use by attempting to modify the technical Internet architecture.

Viewed from this perspective, one can also see that the Internet governance landscape has become an area where there is contention about the role of the different stakeholders, including the appropriate role of governments. Nevertheless, in exploring the evolution and future of Internet governance, the Commission has come to a core conclusion.

Just as the technology radically reduces the barriers that limit people's ability to communicate, to access information, to express their views and to raise concerns, the policy-making process has also, in many jurisdictions and arenas, required greater engagement and become more time-sensitive, and thus more complex and nuanced. We have concluded that in a world of Internet-empowered citizens, effective and long-term stable policy making results when all affected have a voice and method for influencing the process and providing input. We have also witnessed, in the broad range of international regimes influenced by the Internet, that this approach works well while recognizing that in differing policy areas different stakeholders will take natural leadership. But in all areas of concern, ensuring that the positions of all affected stakeholders are engaged and listened to is imperative to ensure stable policy outcomes in a swiftly changing Internet environment. It is this mechanism to which we broadly refer to as multi-stakeholderism, and see as necessary to guide Internet governance going forward.

The Internet We Rely on Is under Pressure

The openness and global connectivity that drives digital innovation and the free flow of information is threatened by the growing interest in exerting control over the use of the Internet or securing a greater market share in the digital economy.[13] At the same time, just as in the off-line world, criminals and terrorists exploit the Internet as an environment that can be used for unlawful ends.

Individual privacy and security increasingly can be threatened by the actions of malicious individuals and also by unthinking, opportunistic or unprincipled corporate and government activities. Public safety is challenged by criminal and terrorist exploitation of the Internet. Financial losses from cybercrime are mounting. Terrorists use social media to recruit youth and propagate their messages. Across every measure, as shown in the polling data in Figure 6, people are very concerned about online privacy and security.[‡] As more personal information is uploaded and shared online, people's digital security is becoming an increasingly important concern. Companies, which rely increasingly on IT infrastructure, are also increasingly affected by cyber attacks, which often result in class-action lawsuits, loss of business, and

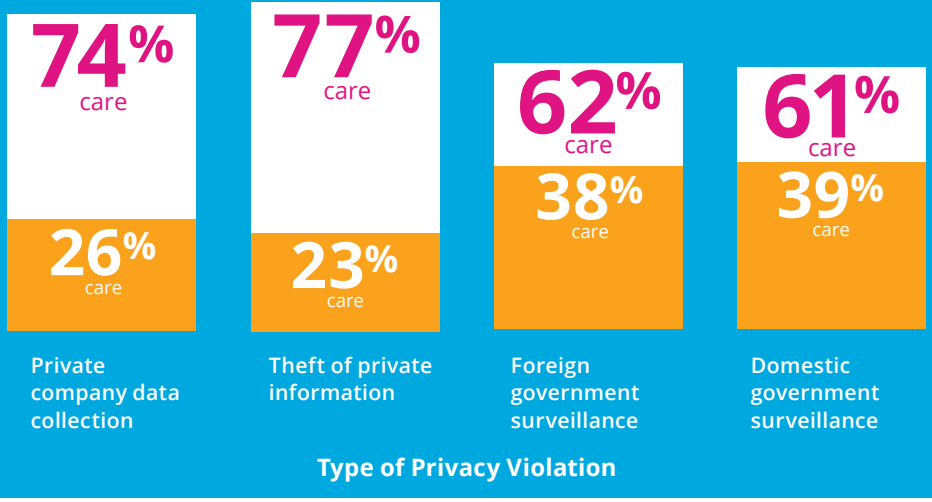
other material and reputational costs. Just a few recent examples illustrate this point. In 2013, companies such as Target, Home Depot and Adobe were hacked. In 2014, all 145 million eBay account holders' emails and encrypted passwords were compromised. And in 2015, the US Office of Personnel Management was hacked and the records of over 21 million people were compromised.

Because of the increased use of digital technologies, the critical infrastructure on which everyday life depends (such as water, electricity and gas) is not just more efficient, but also potentially vulnerable to malicious activities that target both the technology and the services delivered through the Internet. The growing IoT, with billions of connected devices, increases the potential exposure of the public to cyber attacks. The publicity and media exposure of the ways in which the Internet can be used to steal personal data, identities and intellectual property, to launch destructive attacks and to enable excessive surveillance have eroded the trust of users.

We may now have reached a tipping point. Public confidence in the Internet as a trustworthy medium for social and business life is being shaken. From here, we might enter a world where the benefits of the Internet continue to mount. But, it is just as likely that, absent concrete actions from actors across the ecosystem, we could end up in a world where states assert their sovereign control over the network, where private platforms control who benefits from the Internet, or where online criminals dominate the scene. The future depends on the choices we make today. Should these trends continue unabated over the next five years, we could find ourselves entering a period of digital stagnation or decline.

We do not want to throw away the vast opportunities for economic and social advancement that have been gained due to the Internet. To the extent trust in the Internet erodes, global prospects will be damaged, with significant social and economic consequences. Communities will not achieve their potential for educational, social and economic progress. The value creation promised by new and exciting digital innovation will not be realized, including for the next billion citizens of the world who will soon come online. For those in the developed world, increasing inconvenience and financial losses will follow criminal

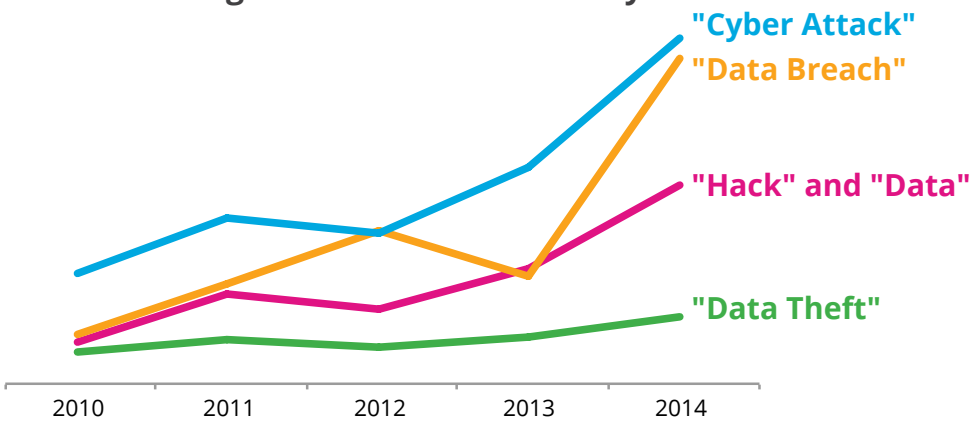
Figure 6: People Care about Privacy Online



Source: Fen Osler Hampson and Eric Jardine, 2016 *Look Who's Watching: Surveillance, Treachery and Trust Online*.[14]

‡ Projections based on technology studies from the MGI, including "Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity" (2011); "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy: (2013); and "The Internet of Things: Mapping the Value Beyond the Hype" (2015). Note that the estimate of the Internet's 2014 economic impact was derived by combining measurement of digital capital and econometric frontier analysis; it encompasses both direct impact and productivity effects.

Figure 7: Media Coverage of Information Security



Source: Samantha Bradshaw, 2015.[15]

exploitation of people's dependency on information and services carried over the Internet. Unrestrained Internet surveillance, repression and censorship will undermine respect for human rights. The potential for new forms of global conflict facilitated through attacks in cyberspace will add tension and instability to international relations.

We Cannot Avoid Risk

Nothing in life is truly risk-free. Every day we make choices in our personal and working lives that have the potential to impact our safety and security. Despite our best efforts, and those of governments, private sector actors and civil society, we constantly face hazards — in everyday life and in the online environment. To date, the benefits brought by the Internet have been underpinned by its open nature (at the technical level) and also thanks to the ease withwhich users can leverage it for economic and social opportunities.

The challenge is to maintain the openness of the Internet while enabling people to manage security risks. The Internet, like any other part of our lives, will never be completely safe, completely secure or completely open. Trade-offs exist, and trying to maximize any of these values will ultimately cause more harm than good. Sometimes the balance between openness, security and safety can become skewed toward one component, causing a reduction in the other two. For example, for much of its early history, the Internet has been heavily weighted toward openness, but this has been accompanied by a lower level of built-in security on the network than might have been specified in its design. The balance is a living one and is always subject to change based upon evolving user behaviour and technological change. This is acutely demonstrated in the challenges we now face as we seek to embrace the enormous potential of the IoT.

We Need to Ensure the Benefits Continue

To move forward, we must appreciate our interdependence and the need for collaborative measures. The risks to our shared digital future can be managed, if everyone plays their part, acting in concert: governments, private companies, the technical community, civil society and individuals.

Our Agenda

The GCIG is convinced it is essential to address the most pressing Internet governance priorities for the next five years. In this report, we begin by recognizing the problems to be overcome. Our agenda builds on existing multi-stakeholder and multilateral initiatives developed to improve aspects of the governance of the Internet, such as the work of the OECD, the UN Governmental Group of Experts, the Internet Governance Forum, NETmundial, the Group of Twenty (G20) and the WSIS, all of which the Commission supports. Yet, it would be a mistake to limit the scope of action to the existing Internet governance forums. The complex of institutions and individuals that have created the modern Internet, and sought to find workable solutions to problems as they arose, have been, and largely continue to be, remarkably successful. However, the Commission is now convinced that the threats to the universally available, open and secure Internet continue to mount. There is a pressing need to deal with the challenges we all face if we want the Internet to continue serving us as the common global resource we have come to know — open, affordable, unfettered and available to all as a safe medium for further innovation.

The Commission has concluded that a normative rather than a prescriptive approach is required to address the kinds of challenges faced by Internet governance. We call on governments, private corporations, civil society, the technical community and individuals together to create a new social compact for the digital age. The Social Compact for the Digital Society will require a very high level of agreement among governments, private corporations, civil society, the technical community and individuals. Governments can provide leadership, but cannot alone define the content of the social compact. Achieving agreement and acceptance will require the engagement of all stakeholders in the Internet ecosystem.

Success in this endeavour will require that we collaborate to refresh and extend the model of multi-stakeholder governance that has thus far empowered the growth of the Internet: to conceive of a new model that embraces greater involvement by those whose lives are affected by governance decisions. This new vision of multi-stakeholderism requires: a more collaborative, global and decentralized model of decision making; enhanced coordination and cooperation across institutions and actors; increased interoperability in terms of identifying and describing issues and approaches for resolution throughout the ecosystem; open information sharing and evidence-based decision making; and expertise- or issue-based organization to allow for both localization and scale in problem solving.

We know that Internet innovation will bring billions of new users online, creating new opportunities, new benefits and new threats. This will certainly mean that our present understanding of who needs to be involved in Internet governance needs to expand and change to accommodate these new interests and new concerned parties. To continue to be effective, Internet governance will need to be more inclusive and more distributed.

We believe this is all possible to achieve in time to avoid the many worst-case scenarios some have posited for the future of the Internet. But we also believe that achieving this vision is only possible if all stakeholders commit to making this new model a reality, through an iterative consensus-building approach to creating a new Social Compact for the Digital Society. We are committed to achieving success, and invite you to join in the process.

To continue to be effective, Internet governance will need to be more inclusive and more distributed.

Transforming Societies and Economies through Access

There is no doubt that access to a secure, open, trustworthy and inclusive Internet is fundamental for transforming future societies and economies. But *access* is the first fundamental step for realizing all the benefits the Internet can bring to commerce and innovation, creativity and expression, and communication. The Commission believes that the Internet is for everyone. Achieving a truly universal Internet is fundamentally about equity, and success will depend on the complementary efforts of governments, the private sector, the technical community and civil society. Success must not only be measured by the number of people connected, but also by the quality of the Internet to which they gain access. Commitment to expanding access must be accompanied by a commitment to maintaining an open network that equally provides all users the ability to access, use and create knowledge in a non-discriminatory environment, free of arbitrary censorship or unjustified controls.

Internet access can be understood as the set of devices, services, facilities and skills that allow people to connect to and use Internet services, applications and content. Achieving the widest practical access has become a priority for policy makers and regulators around the world, and is a core pillar of the United Nations Sustainable Development Goals (SDGs), which recognize the need to "[s]ignificantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020" and to "enhance the use of enabling technologies...to promote women's empowerment."[16]

Historically, access to the Internet has been uneven, although it continues to expand apace. One reason for this accelerating rollout is the increasing awareness of governments that competition and private capital can be used to expand Internet access, augmented by

UN SDGs

Source: United Nations. https://sustainabledevelopment.un.org/sdgs

applying regulation or public funds where there are insufficient commercial incentives or competition. Barriers to Internet access can exist for a number of reasons, including a lack of Internet infrastructure, a failure to implement technical standards that promote access for the disabled, a lack of competition and some rigid regulatory approaches leading to unaffordable pricing schemes for some potential users, or limited digital education and literacy. While new technological capabilities continue to assist in addressing the barriers by some, inequalities in access, affordability and skills have excluded others from reaping these benefits. Some groups of people face more daunting barriers than others.

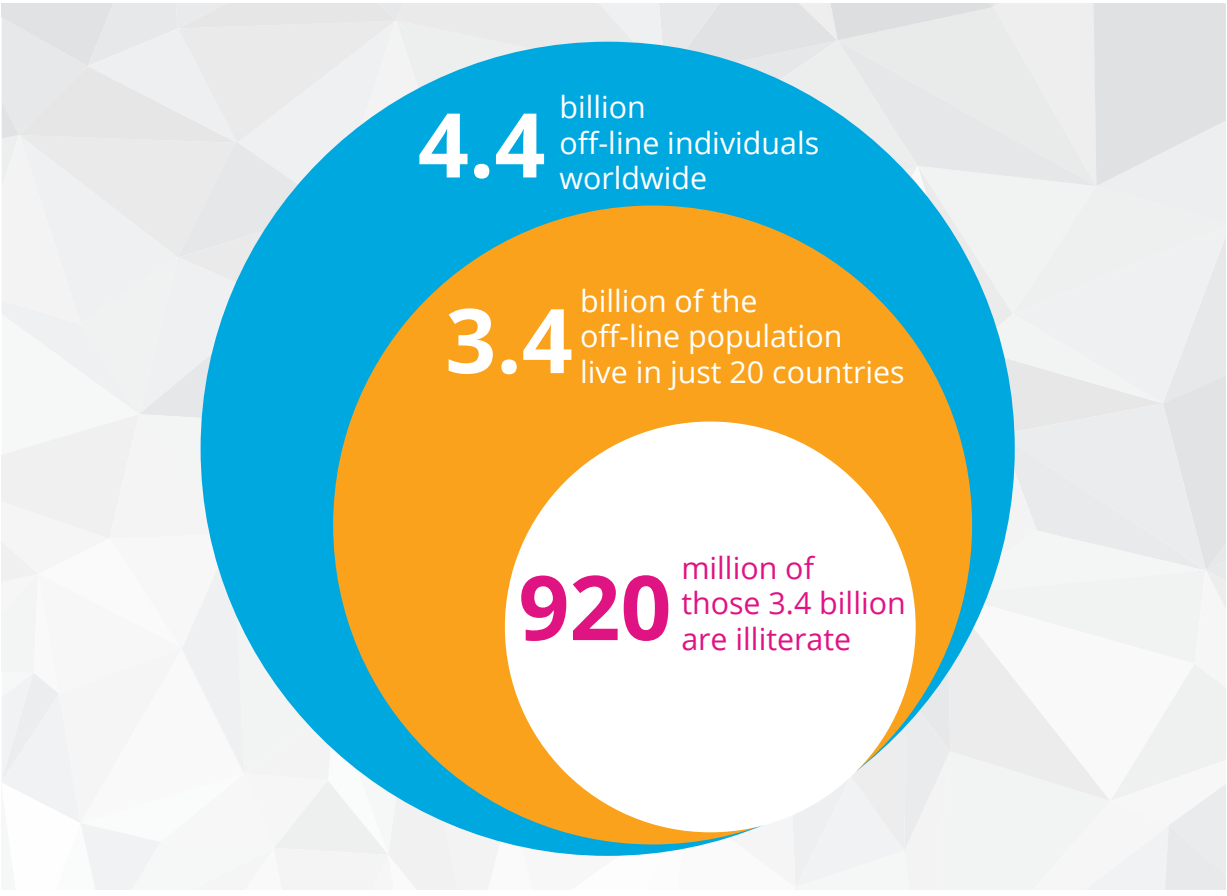
The gap in Internet access — for technical, political, economic or social reasons — has been described as the digital divide. The divide exists within and between countries, between the rich and the poor, between rural and urban populations, within families, between the young and old, between men and women, and between the abled and disabled. More than 60 percent of the world remains off-line and without removing critical barriers to adoption, four billion people could be excluded from the digital economy. Roughly three-quarters of the off-line population live in 20 countries. Those that are unconnected disproportionately live in rural and remote areas, have low incomes, and are illiterate and female.[17] Closing these divides and ensuring that all people have the necessary skills and tools to access and use the Internet is necessary for promoting economic prosperity, preserving cultural values and historical records, empowering individuals and achieving development. Research has shown that an increase in a country's Internet maturity is correlated with a sizable increase in real per capita GDP.[18]

An enormous amount of economic and social value is realized when one has the ability to use the Internet. Connecting the unconnected and promoting a secure, inclusive, trustworthy and open Internet is imperative to empowering individuals no matter their age, gender, abilities, skills, income, location or identity. All stakeholders have a responsibility to do their part to ensure that "the Internet for all" is more than an empty phrase. How can we bridge the divides that exist within and between societies so that the Internet can continue to be an open platform that empowers individuals and promotes human rights, cultural preservation and economic innovation for all segments of society?

Current Challenges: Achieving an Internet For All

By the end of 2015, four billion people remained off-line. This means only 43 percent of the world's population is online with some form of regular access to the Internet. The gap is especially pronounced in the transforming societies where upward of 65 percent of the population is precluded from participating in the digital society. And in some of the world's poorest countries, only one in 10 people is online.[19] That being said, such divides once seemed at least as daunting in terms of expanding connection to the telephone network, yet those barriers were overcome by the

Figure 8: A World of Digital Divides



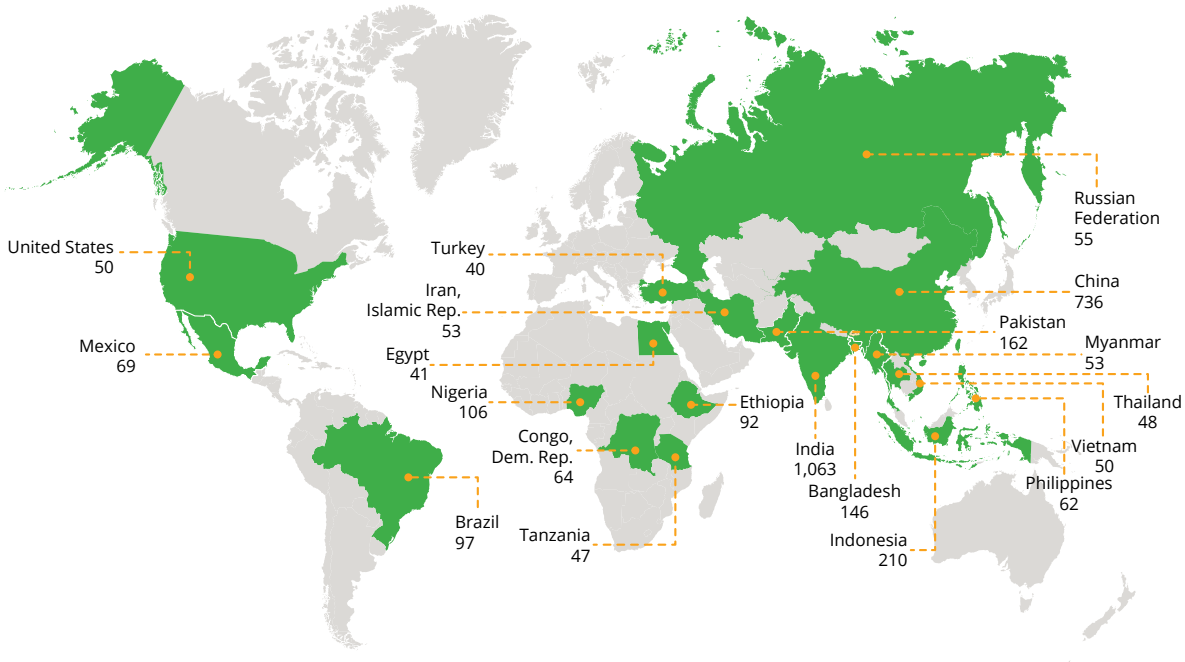
Source: "Offline and Falling Behind: Barriers to Internet Adoption," McKinsey Technology, Media and Telecom Practice. [20]

adoption of policy and regulatory reform to harness commercial and technological opportunities. The Commission believes the same can be true for the Internet.

The ways in which people access the Internet have changed over time. Initially, Internet access was largely facilitated by the use of personal desktop computers and fixed-line Internet connections into universities, homes, offices and public facilities. More recently, Internet-capable mobile telephones (smartphones) have begun to play a much larger role in facilitating Internet access, especially in transforming societies. It is now predicted that the next billion people to connect to the Internet will gain access through mobile devices. With its integration into mobile, the Internet is continuously evolving, offering exponentially more tools and applications to improve people's livelihoods and overall quality of life. In Africa, for instance, mobile networks have provided the platform for bringing financial services to millions who were previously excluded from the formal banking system.[21] There is now a large body of research that demonstrates the importance of affordable broadband connectivity for social inclusion, civic participation and environmental protection. It is also an enabler of economic growth. A recent study documenting the rapid expansion of e-commerce in China found that approximately 40 percent of online sales did not merely replace off-line transactions, they actually unlocked incremental consumption.[22]

Expanding Internet access, made possible by the adoption of smartphones and wireless broadband, will be the major means by which new users will access the Internet and participate in the networked society. However, the ability for any country to take advantage of wireless capabilities relies on pervasive fixed networks, which enable backhaul of traffic. In developed countries, the bulk of smartphone traffic uses Wi-Fi connected to fixed lines in homes and offices. Thus, mobile access depends on the quality and availability of fixed communication networks. To make the most economical use of the scarce radio frequency spectrum allocated to them, mobile operators try to hand-off wireless data to the fixed networks as soon as possible. Accordingly, the spread of the mobile Internet

Figure 9: The Internet's Uneven Footprint



Source: "Offline and Falling Behind: Barriers to Internet Adoption," McKinsey Technology, Media and Telecom Practice. [23]

ultimately remains dependent on the availability of substantial investments to grow the fixed network. This calls into question how far the unconnected will be able to quickly "leapfrog" in their penetration rates.

Alarmingly, there are still some indications that the rate of Internet expansion is stagnating in parts of the world where growth is needed to bring new users online. A number of different challenges stand out: prices for mobile Internet access remain high in many locations and strategies to improve coverage and connectivity in rural areas will frequently be different than those needed in urban centres; culturally relevant content and services are needed to demonstrate the value of the Internet for potential users; and digital literacy needs to be enshrined by governments to educate policy makers and the wider public on the value and potential of the technology.

The Internet continues to be a tool that enables the transformation of societies and economies, and has led to new innovations for governance and development. Like the Internet itself, development strategies for transforming societies are becoming more distributed. While this poses opportunities for expanding access through distributed local infrastructure or peer-to-peer sharing, there is also risk as decentralized agency and innovation weaken traditional state institutions (some of which are already weak). Legislators, regulators, private companies, the technical community and civil society can each play an important role to bridge current gaps and prevent new ones from growing, so that the four billion people who still remain off-line are given both an opportunity and a choice to fully participate in the networked society.

Infrastructure Capacity

The Internet requires different physical equipment to operate: cables, routing equipment, servers, satellites and their accompanying terrestrial infrastructure, fixed and mobile access networks and exchange points are all necessary in providing an Internet connection. In order to gain access to the Internet, continental infrastructure needs to be connected via submarine cables; landlocked countries need terrestrial fibre and mobile towers; and additional IXPs, which provide connection points for Internet traffic to move between networks, need to be built to exchange traffic more efficiently and affordably domestically and internationally.

However, the construction and expansion of physical Internet infrastructure has not occurred to the extent necessary to bring all people online: many small island states still lack submarine cables and must rely upon generally more costly and inefficient satellite connections; many landlocked countries do not have enough fibre optic cables connecting them to neighbouring countries and regional Internet hubs; and many countries do not have traffic interconnection facilities such as IXPs, increasing the cost and latency for transmitting data across networks. As Pablo Bello and Juan Jung note in their GCIG paper, there have also been dramatic changes in consumer patterns that are increasing the demand for data.[24] These inequities are especially pronounced in rural or remote areas, where challenging geography and low population density limit the potential for investment. Even where some connectivity exists, users may face higher prices reflecting higher costs or a lack of competition.

It can be expensive to build and operate some parts of the Internet infrastructure due to the cost of equipment; the growing difficulty to deploy networks to reach those who are still not connected, often located in rural or remote places; and the need to upgrade networks to accommodate the growing pace of technological change. Outmoded or poorly considered legislative and regulatory instruments sometimes exacerbate all of these factors. Unnecessarily high costs are eventually passed on to the user, but service provider charges may also be excessive if they are not disciplined by competition. It is thus essential for governments to create legislative and regulatory frameworks that encourage the investment in physical infrastructure necessary to improve and expand Internet access, as well as to promote competition and remove barriers to reduce costs.

A number of strategies are known to stimulate infrastructure development: barriers to investment can be reduced or removed by regulators; radio frequency spectrum can be allocated under conditions

Recommendation

Regulators should put in place measures to encourage competition and foster investment in networks as fundamental requirements in any effort to enable access and promote development.

Recommendation

Efficient network interconnection and traffic exchange are essential to improve access and affordability of broadband. For this purpose, IXPs should not be captured by any one interest, whether by governments or a private company, to further their own benefit at the expense of others. They should be neutrally operated and governed by shared agreements among the relevant stakeholders.

Recommendation

Government should invest in public access points, which can play a significant role by providing individuals with an opportunity to connect to the Internet. The installation of public Internet access points should be encouraged in schools, libraries and other social service venues to ensure that individuals are not prevented from having access due to a lack of tools or available resources. In some instances, central, state and municipal governments may consider investing in the build-out of access networks, again, for the most part, where private sector investment is insufficient.

Recommendation

Governments should facilitate network sharing. Other cost-sharing initiatives can help to work toward achieving universal access, for example, by encouraging firms to take advantage of infrastructure projects such as building roads and power lines to reduce the cost of laying fibre optic cables as a way to connect rural populations. However, network sharing should encourage competition and not serve as a disincentive to investment or contribute to the creation of monopolies.

providing incentives to meet coverage objectives; and universal service funds can be established to fund public subsidies to complement private investment in expanding access. Governments and private companies can also work together to promote the sharing of networks and laying fibre optic cables in conjunction with other infrastructure-building projects, such as roads and power lines. Research has demonstrated that infrastructure sharing can improve connectivity, reduce the cost of building out the network infrastructure, generate more revenue, improve retail competition among operators by reducing the barrier to entry and, ultimately, reduce access costs. However, regulators must be vigilant to not discourage investment or contribute to the creation of monopolies in promoting the sharing of networks. Experience has proven that competition brings down prices and encourages innovation, particularly in mobile communication. The same is true for Internet access. The more this is encouraged, the more access will increase. At the same time, public policies must foster network investments to close the coverage gap and increase capacity.

Affordable Internet Access: Pricing and Commercial Flexibility

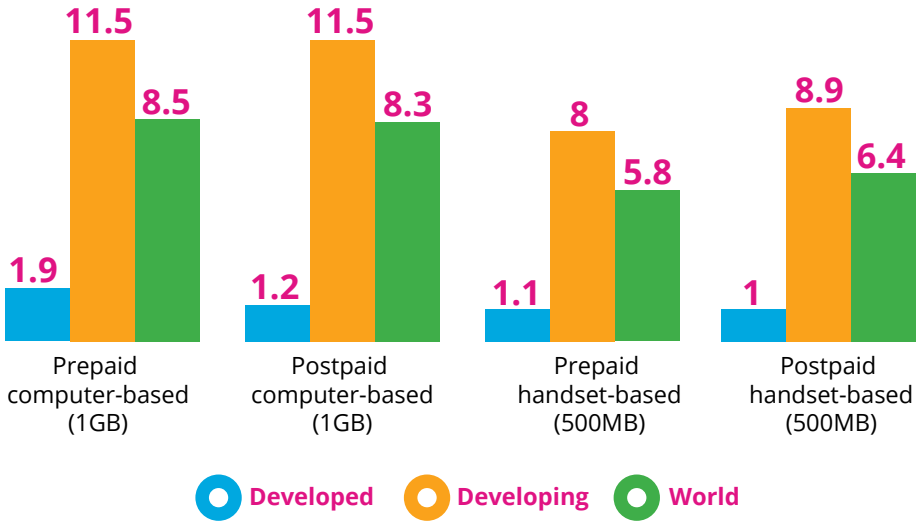
Beyond the high cost of infrastructure, there are a host of other factors contributing to a lack of affordable Internet access, which remains a major barrier to bringing the next four billion people online. Many people, especially the world's poorest, are prevented from accessing the Internet by a combination of high costs or low incomes. Women, on average, have lower incomes, and in some situations, have less control over spending; therefore, they can be disproportionately affected by affordability.[25] A recent study found that

the world's women have only 84 percent of the access to the Internet and mobile phones that is currently enjoyed by men.[26] Despite the downward trend in prices,[27] for many households in transforming societies a fixed Internet connection remains unaffordable. While innovation in the pricing of mobile broadband services has allowed more people from lower income groups to connect to the Internet, mobile connections can still take up a large percentage of an individual's monthly income, ranging anywhere from 8.9 to 11.5 percent as a percentage of gross national income (GNI) in transforming countries (see Figure 10).[28]

Reaching people with lower incomes or in more remote areas will require competition to allow market forces to drive Internet access in the same way it has for mobile telephony. In the mobile telephony market, competition has inspired innovative pricing plans that enable users to afford and control expenditure (for example, pre-paid services). The majority of Internet access, particularly on fixed networks in developed countries, is provided for a set monthly price irrespective of the amount of data a user sends and receives or is charged according to the speed selected by a user (i.e., faster speeds are billed at a higher price). Often, the traffic sent and received over the Internet using mobile networks is metred or provided to users with a cap on the amount of data (bit cap) that is provided at a given price. However, in some countries, businesses offer unmetred traffic for specified sources of content. This is referred to as "zero-rated content" and has been used for many years in some countries, or "sponsored" content, which has more recently been cited as a potential way to expand Internet access. In the absence of sufficient competition, however, these schemes raise a number of concerns around the potentially negative effects they may have on the future development of innovation in the digital ecosystem. For example, if one source of content is zero-rated and others are not (and therefore are more expensive to access), competition could be stifled. In particular, new firms could be prevented from entering the marketplace.[29]

In contrast, in some markets typified by low bit caps there is a potential for zero-rating to increase competition. This occurs where there is a dominant player or a small number of players controlling the backbone market. In these cases, other Internet service providers (ISPs) and content providers can band together to reduce their individual costs (called peering), thus bypassing the less competitive part of the market. By

Figure 10: Mobile-broadband Prices



Source: International Telecommunication Union (ITU), 2014, "Measuring the Information Society.[30]

reducing their transit costs they can pass these savings on to their customers with unmetred access to specific services (for example, an online radio station that peers directly with an ISP).[31] Concerns about zero-rating arise where there is either insufficient competition or it is used in an anti-competitive manner.[32] Regulators must be vigilant to prevent such negative effects.

Others debate the costs and benefits of zero-rating for different reasons. The practice of zero-rating has been increasing in the transforming societies, where popular Internet services such as Facebook, Twitter, Wikipedia and Google have partnered with some ISPs to offer access to their content. It is important to note that these services do not offer access to the full Internet, only to a limited number of websites. On the one hand, such practices may benefit some users who may otherwise not be able to afford access, and thus potentially generate broader economic and social externalities, such as through offering access to websites that contain information related to education, health and public services. Proponents also say such access could stimulate demand for further usage, including content not part of such schemes, and thereby potentially expand the purchase of paid Internet services. On the other hand, any such arrangements advantage the use of some consumption or creation over others, with those choices not normally being made by users. Furthermore, zero-rating also treats Internet users strictly as consumers of content, and generally does not take into account that the ability to create and distribute content, outside the coverage of these schemes, is a fundamental part of the use of the Internet.

Private sector content providers can play a large role in helping bridge divides by developing alternative, innovative pricing models that promote access to certain content. While these models are in the early stages of development in some countries, more innovative policies are needed to give some of the world's poorest an opportunity to participate online. However, regulators should ensure that zero-rated schemes do not distort the competitiveness of the market, either by giving preference to some content providers over others or by distorting price mechanisms. Pricing models, including mixed free and paid models, must adhere to principles of openness, security, transparency and fair competition to prevent any harm to competition and innovation within the digital ecosystem.

Governments can also play a role in making access more affordable by creating a regulatory environment that opens up markets and encourages competition in commercial pricing. Around the world, there is already a large body of evidence that demonstrates that competition helps decrease costs for the user. For example, the ITU found that "in developing countries, fixed-broadband prices could be reduced by 10 percent and mobile-cellular prices by 5 percent if competition and/or the regulatory framework is improved."[33] As affordability is an issue that affects the world's poorest, governments can reduce or eliminate any industry-specific taxes on services and equipment they may have in place, and thus assist in reducing costs. This is not a call to reduce or eliminate taxes applied across an entire economy in a neutral manner, such as a value-added tax (VAT) on Internet access. Rather, as competition and the elimination of industry-specific taxes (for example, SIM card registration) reduces prices, it will stimulate demand and increase the returns to the public purse through increased volumes.[34]

Foregoing taxes on the most inexpensive range of access devices, such as smartphones or tablets, could be considered as part of a program to boost Internet take-up. It is critical that this take place only in a competitive market; otherwise, players may raise prices to the level prior to the reduction, thus defeating the goal. Generally, however, taxes should be applied in a neutral manner as any differences in rates, such as between generations of mobile technologies (i.e., 2G vs. 3G), may provide an incentive not to acquire a

Recommendation

Regulatory authorities should ensure that these services adhere to principles of openness and fair competition. In the absence of sufficient competition to enable consumer choice, there should be no exclusive agreements to provide zero-rated content.

device with Internet access. Industry-specific taxes such as those for SIM card registration, which add to the burden of neutral taxes, should be eliminated. Similarly, there should not be tax breaks on specific access plans. Tweaking the tax rates applied to specific plans can often distort how these plans evolve and can actually act as a limit on meeting goals. If governments wish to provide subsidies to consumers, these should preferably come from general revenue in a transparent and neutral manner, to ensure the benefit is passed on to the intended beneficiaries. These subsidies should be equally available to all competitors in the marketplace to not stifle competition. Finally, as competition lowers prices, it also reduces the tax burdens of instruments such as VAT. Typically, any reduction in government revenue resulting from lowered prices is compensated for by increased market size, volumes and other factors. In addition, neutral taxes do not distort the market in the same way as industry-specific taxes. For example, the level of tax applied to SIM registration, introduced for mobile phones, may depress the use of SIM cards for IoT devices, which have entirely different average revenue levels.

While the cost to connect to the Internet is generally decreasing worldwide, affordability must remain an explicit goal — one best achieved by fostering competition. Experiments with zero-rated services to provide limited access and other alternative pricing schemes for providing basic access to some Internet content, may be of some benefit for connecting low-income populations to the Internet.

Affordable Internet Access: Devices

Another important consideration for expanding connectivity is the cost of devices used to connect to the Internet. In order to achieve an Internet for all, new users must have access to affordable devices. Without affordable devices (such as smartphones, personal computers or laptops) it will not be possible to bridge the digital divide. Policies such as customs duties, tariffs or import quotas can increase the final prices of devices. The lack of commercial flexibility that may prevent ISPs from offering plans that offer discounts on devices, can also hinder acquisition. That said, such practices can come with their own set of issues, including the duration for contracts or potentially more expensive outcomes for users, including those that purchase their device separately. This is why promoting choice for users through tools such as competition is critical along with the flexibility for commercial offers to evolve.

Recommendation

Governments need to ensure their taxation policies do not bias the market for Internet services or related equipment. Telecommunication, Internet access and usage should be taxed at the same rate as other services. If governments want to provide subsidies and incentives to consumers, they should be done in a transparent and neutral manner rather than through the taxation system.

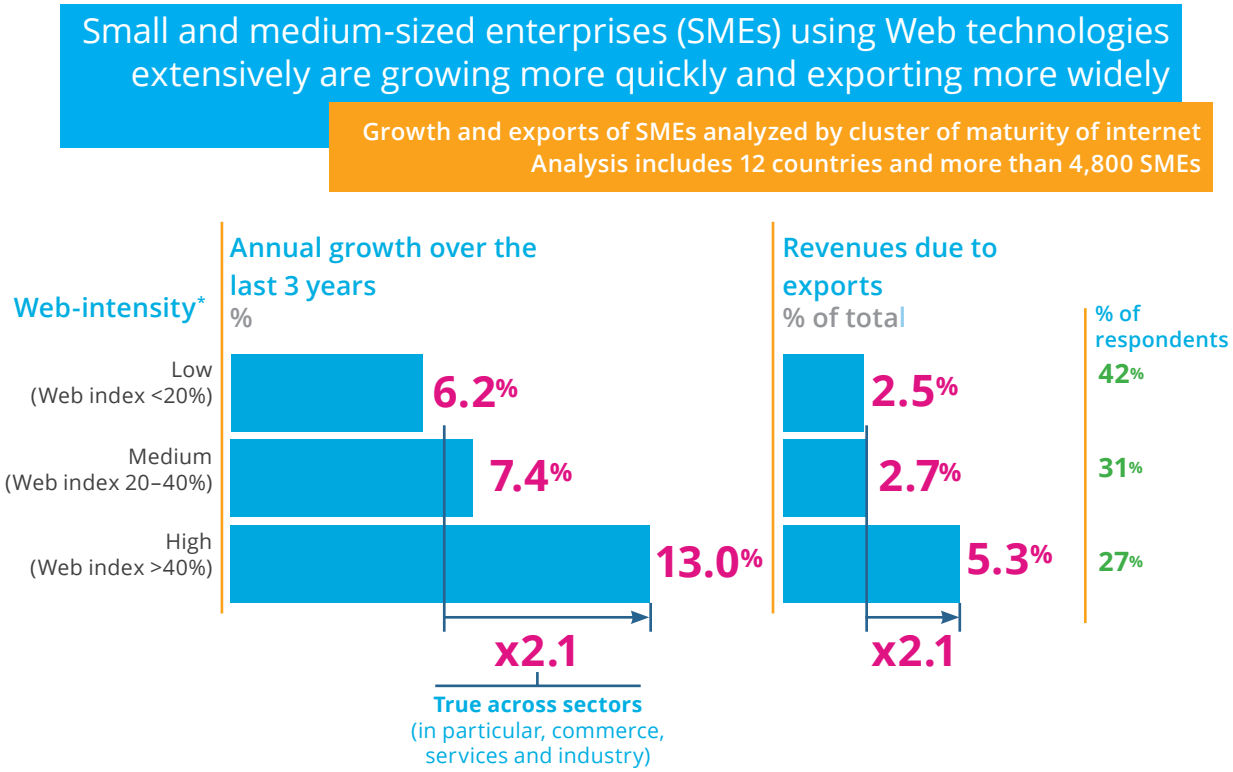
Recommendation

Governments should fully use the tools at their disposal to promote competition among the producers and sellers of devices to increase affordability, whether purchased separately or as part of service plan.

Recommendation

Development assistance agencies, civil society organizations or other actors can also help make devices available to the poorest segments of the world's population by creating special programs that help provide the devices necessary to connect to the Internet.

Figure 11: The Web as Small and Medium-sized Enterprise Multiplier



*McKinsey Web index defined according to the number of technologies possessed by companies and the penetration of those technologies (i.e., the number of employees/customers or suppliers having access to those technologies).

Source: "Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity." McKinsey Global Institute.

Some countries have developed special programs to lower the costs of devices for low-income users. For instance, Colombia offers a general tax exemption on devices in the lower and medium price range. In addition, it gives subsidies for users in the lowest income bracket, which can be used either for buying a device or paying for a broadband connection. Other countries have developed programs that provide users with free devices, such as Uruguay's One Laptop per Child program. In addition, the private sector has been developing a broader range of less expensive devices in recent years, especially in markets where the level of competition is high between different device makers.

Human Capacity

The Internet stimulates creativity and makes available new opportunities—including opportunities that were once out of reach for individuals and entrepreneurs. As the global economy grows increasingly digital and more interconnected, the Internet has become an essential tool for job searching, networking, conducting business, receiving and making payments with buyers and suppliers, and accessing microcredit.

The wealth of knowledge that can be accessed online can be used to improve all aspects of human well-being. However, it is important to remember that Internet access is not just about providing infrastructure and devices. People also need literacy, knowledge and skills to use the Internet to its full potential. Basic digital literacy is increasingly a required skill for

better-paying and more productive jobs. Many simply lack an understanding of the technology or a sense of how it could be relevant to their lives. Others will not use the Internet or services offered on it because they are concerned about privacy and surveillance issues, or they are afraid of cybercrime. Education about the dangers users face and how users can best protect themselves is a vital component of capacity-building efforts.

Innovation can be a bottom-up process. Once individuals are given the tools, they are likely to be the most creative in addressing the problem of unmet local demand. The power of demand-driven innovation at the local level is well exemplified by the development of platforms to allow mobile telephones to be used for money transfer in countries without well-developed or broadly used banking systems.

Transforming economies play an important role as producers in the Internet economy. Their unique experiences provide them with opportunities to innovate in ICT and related Internet applications. Transforming societies are not solely consumers of Internet technology, but also play an important role in the production and design of Internet and mobile applications to meet local needs and, sometimes, to serve global markets. Corporate competition has been dramatically intensifying as Internet platforms and e-commerce marketplaces lower costs and barriers to entry for thousands of small firms from emerging economies. They are increasingly able to obtain the resources and global exposure required to compete with established industry incumbents from advanced economies, building on their intimate knowledge of local customs and needs.[35] Ensuring that individuals are given the skills and tools to innovate and governments promote a regulatory environment that encourages ICT start-ups will be essential to unleashing digital innovation and entrepreneurship in the transforming societies.

Finally, it is important to recognize that demand factors are just as important as supply factors in explaining current adoption trends, and bringing new users online. According to Hernán Galperin's GCIG Paper No. 34, which examines trends in Internet access and use in Latin America, although users in rural areas had access to needed infrastructure, "the majority of nonusers simply found existing services too expensive or irrelevant."[36] Thus, it is incredibly important that all stakeholders play a role

Recommendation

Governments, in collaboration with other stakeholders, should emphasize the value of Internet connectivity and promote demand for Internet content. This necessitates developing people's capacity to use e-services, such as e-health, e-government and e-learning.

Recommendation

SMEs play an important role not only in creating valuable local content, but for driving the development of transforming nations. Governments should help to educate software engineers and local content providers so that they can develop businesses that can compete globally and content that will encourage local demand-driven Internet usage.

Recommendation

Governments should promote digital literacy programs in schools and within government organizations. For government officials, the Internet has become an important tool to carry out their duties, the subject of concern that may require legislative or regulatory responses, and even for international outreach and diplomacy. It is vital that policy makers understand the foundations of the technology and the principles that must be maintained in order to preserve the Internet as a tool for innovation, communication and the enjoyment of rights.

in emphasizing the value of connectivity and create online platforms that are tailored to the specific needs of their respective constituencies, as well as providing them with the tools to develop their own applications and services to meet local requirements.

Inclusion

The Internet offers an opportunity for greater inclusion of often marginalized groups. Achieving universal access to the Internet means ensuring no one faces barriers to access based on attributes such as their age, race, gender, culture or ability. Priorities should include linguistic inclusion and the inclusion of people with disabilities.

As the next four billion people come online, language will be a major barrier to inclusion. Many people are not aware of the Internet's potential, or cannot use it in a way that is meaningful to them, because there is no useful content available in a language they can understand. In order to connect everyone, it is vital to increase the representation and availability of content in a wide variety of languages and scripts.

Language is not the only barrier to inclusivity. When it comes to the Internet and the various applications made available through new technologies, people with disabilities face different barriers. Surveys conducted by the World Health Organization have found that persons living with a disability are half as likely to have a computer at home, and even less likely to have an Internet connection.[37] This is troubling, as the Internet can open up new economic and social horizons for people living with disabilities that might not have been possible before. The Internet can provide access to all kinds of health, education, transport, government and services information. Individuals can access health-related information or services, local and global markets, or Internet forums. Online communities can provide opportunities for individuals to share

INTERNET ACCESS FOR REFUGEES

The United Nations High Commissioners for Refugees (UNHCR) estimates that refugees spend an average of 17 years in exile.[39] This figure represents the average number of years refugees are displaced and in need of assistance before they can safely return home or find refuge in another country. The UNHCR also estimates that there are currently 60 million displaced men, women and children as a result of continuing crises around the world.[40] According to the UNHCR as of 2015, 51 percent of refugees were under 18 years old, which represents the highest figure for child refugees in more than a decade.[41] Technology can help alleviate some of the suffering that individuals face in refugee camps for extended periods of their lives. In addition to being a critical connectivity tool through which refugees can communicate with family members, the Internet is an essential tool of twenty-first century commerce that allows displaced individuals to put to use their entrepreneurial skills and eventually lessen their dependence on aid. Access to online information is also a crucial engine of learning and human development. While the role of teachers is essential, access to online education is a very important tool to ensure refugees can continue their education while dislocated. The less disconnected refugees are, the easier it would be for them to reintegrate back into societies, whether in their countries of origin or in other destinations.

Recommendation

It is therefore imperative that refugees be provided access to the Internet by host governments or as part of an aid package from international donors. Host governments, specialist agencies or non-governmental organizations should also ensure access to online education and entrepreneurship courses, and support sites to ensure the continued human development of refugees.

their experiences and build support networks across diverse cultural and geographic contexts. Accessing general information and being able to participate in online communities can be an incredibly empowering experience, as it enables people with disabilities to overcome any potential physical, communication and mobility barriers.

While there have been many positive developments in terms of making technology accessible and developing programs and applications for blind, deaf and hearing impaired people, there are still many challenges. "Persons with disabilities face as many different barriers as there are types and degrees of disability. For example, people with a visual impairment who use screen-reading software may be confronted by websites that have confusing navigation, or that lack descriptions of images; while people with a hearing impairment may be unable to participate in online conferencing because it lacks captioning."[38] The Commission believes that people with disabilities should have choice in Internet technologies and communications devices equivalent to that available to other people — in terms of access, quality and price. Addressing these challenges will require raised awareness of these issues, innovations in technology, development of common standards and a regulatory environment that promotes access for those with disabilities. Access issues related to disability are important issues that affect us all. While we might be able to make full use the Internet now, this can change over time, especially as we age. It is vital that policy makers and regulators make inclusion a policy priority.

Measuring Access

Having access to high-quality and timely information is vital for guiding appropriate policy responses. Knowing who is connected in aggregate terms, how they are connecting and the effects this connection has on people's lives, can help all stakeholders not only address divides in access, but also improve the quality of connection and the relevance of policy. Yet, for many parts of the world, the metrics used to measure Internet access are not up to date and not available in a timely manner. Consistent metrics for measuring access and processes for ensuring that data collected is current and reliable need to be developed.

Recommendation

Governments play an important role in increasing access for persons with disabilities through their respective legislative processes. Open technical standards that promote access for persons with disabilities should be incorporated into procurement policies, with adherence a requirement for hardware and software.

Recommendation

Governments should provide incentives and appropriate regulation to encourage private-sector hardware manufactures and software developers to include accessibility standards in their products. Non-governmental organizations and technical consortiums that develop these standards should also be encouraged to continue to develop them.

Recommendation

Current information is vital for guiding appropriate policy responses. National statistics agencies should actively collect information on Internet access. Governments should invest more resources and work in cooperation with the relevant stakeholders — such as the 14 members of the Partnership for Measuring ICT for Development, the G20, universities and other regional organizations — to define consistent metrics for measuring access and processes for ensuring that data collected is current and reliable.

THE PARTNERSHIP FOR MEASURING ICT FOR DEVELOPMENT

The Partnership for Measuring ICT for Development (ICT4D) is an international, multi-stakeholder initiative to improve the availability and quality of ICT data and indicators, particularly in transforming societies. The ICT4D was formed in 2004, as a collaborative forum for the United Nations and other agencies, to address challenges of data collection and analysis concerning ICT4D and WSIS outcomes. The partnership has 12 member organizations: the ITU, the OECD, the UN Conference on Trade and Development, the UN Department of Economic and Social Affairs, the UNESCO Institute for Statistics, the World Bank, the UN Economic Commission for Africa, the Economic Commission for Latin America and the Carribean, the Economic and Social Commission for Asia and the Pacific, the UN Economic and Social Commission for Western Asia, and Eurostat, and the UN Environment Programme Basel Convention Secretariat joined in 2011.

Ensuring Human Rights for Digital Citizens

Our understanding of human rights has entered a new era with the creation and rapid spread of the Internet. The Internet brings unprecedented reach to certain fundamental rights, such as freedom of thought, opinion, expression and assembly. Similarly, the right to participate in governance, to receive an education and to participate in cultural life, the arts and scientific advancement and others have gained new meaning, and new effect. These effects are tremendously positive, but it is also possible to use the Internet to the detriment of others. Examples include the ability to interfere with an individual's privacy and correspondence, to attack an individual's honour and reputation, or to deprive creators of the reputational and material benefits resulting from their creations. The Internet has also given rise to new threats to the security of individuals, corporations and the state itself. All of these powerful positive and negative developments taken together represent significant new governance challenges.

New challenges to international human rights are requiring governments and policy makers to confront and sometimes to regulate the use of a technology that is, in many ways, immune to national statutory and particular cultural contexts, as it transcends national borders. The UN Human Rights Council has taken a strong stand to say that the same rights people enjoy off-line must also be protected online. But the specific challenges presented when trying to implement that position still remain to be addressed. There has not been a direct translation from rights off-line to rights online: states and corporations actively collect information about individuals, often without their knowledge, informed consent or full understanding; Internet content is censored or controlled for various purposes, some of which may infringe on an individual's right to freedom of speech; and online platforms are sometimes monitored and used by governments to limit freedom

of expression, assembly and religion. There are also important questions concerning the vulnerability of interconnected systems and the privacy implications of allowing state and private sector actors to access, benefit from and share the immense amounts of data that they will generate. Similarly, there is a need to clarify that whatever access is granted must have a legal basis.

This section addresses some of these challenges by developing and articulating norms for digital citizenship, as well as reasonable expectations of governments. Taken together, broad acceptance of these norms can generate respect and protect fundamental freedoms, promote innovation and economic growth, strengthen security and promote the continued resiliency of the Internet and future technologies.

Government Surveillance, Privacy and Security

Personal, commercial and public sector information is increasingly easy to access by legal means, as are Internet-connected devices. This development creates opportunities for innovation, growth and prosperity, but it also introduces new challenges. These are magnified by the growing use of mobile devices and wireless networks that offer additional ways for networks to be penetrated. Many businesses in every sector now depend on big data and algorithms. Creative ways of treating personal data such as health records are often those that can offer the most significant social benefits, such as helping to pinpoint the right medical treatment, but consumers are wary of how their most sensitive information may be used. Additionally, the advent of the IoT is already starting to connect the most basic objects and instruments of daily life — our homes, our appliances, our cars, our clothing and much more. In the emerging world of the IoT, everything we do, see, use or touch will have the potential to leave electronic tracks. While the potential commercial and social value of such data is immense, many challenges will have to be addressed to realize the benefits.

Our communications and associated data are mixed together in the packet-switched networks and data clouds of the Internet. They all use the same fixed and mobile devices operating with the same Internet protocols. For authorities charged with tracking down criminals or terrorists, the Internet provides a reservoir of information about their targets. But at the same time, access to the intermingled data raises concerns over personal privacy, data protection, digital security and business competition.

Governments have the responsibility to ensure that the Internet policies they pursue are consistent with fundamental human rights and the rule of law. At the same time, they have a duty to address threats from both state and so-called "non-state" actors such as terrorists and criminals of all kinds. However, it is sometimes difficult for law enforcement officials to indict and prosecute national and transnational criminal activity without having assistance from intelligence agencies and their powerful tools of digital intelligence gathering.

Complicating matters further, government data and activities themselves are vulnerable to terrorists, cyber criminals and other states through the Internet. Many governments are seeking to work with businesses to improve national cyber security to counter cybercrime, and the manipulation, disruption and destruction of critical national infrastructures. These increased risks underscore the importance of governments monitoring cyber threats. Nevertheless, some governments are conducting surveillance for purposes and in ways that have a negative effect on fundamental human rights such as privacy, freedom of expression, and legitimate dissent and protest.

The development of the Internet and its absorption into every aspect of our political, economic and social lives have provided new methods and opportunities for government surveillance. As communication of all types of data moved to Internet-based transmission, the opportunities for intelligence agencies to monitor targets by intercepting and exploiting digital data increased. This so-called "data revolution" has not only changed how surveillance is being conducted, but also what can be monitored and for how long. The Internet has facilitated the retention of large amounts

METADATA VS. COMMUNICATIONS DATA

The Internet and applications that are deployed on it have created new challenges for law enforcement agencies to gather evidence for prosecuting criminals. Police and other law enforcement actors have traditionally used "communications data" as evidence to track the movement and contacts of criminals. Now that the majority of our phones are connected to the Internet, a wealth of additional, transactional metadata is also created by our mobile devices. Legal thresholds for lawfully authorized access to communications data must be redefined to ensure that the aggregated collection of metadata — such as an individual's full browsing history — are treated with the same respect for privacy as access to the actual content of a communication, and should only be made under judicial authority. In all cases, the principles of necessity and proportionality must be applied.

of transactional data about individuals. This "data about other data" or "metadata" includes information such as an individual's location, their browsing and viewing habits, contacts and communications, or their online purchasing habits. When correlated and analyzed, this information can provide an extremely detailed picture of a person's life that is more intrusive than what would have been possible through the use of communications data alone — who called whom, when, where and for how long — that is available from a traditional itemized telephone billing record or pen register.

As the next section will discuss, the concerns about vast data collection, aggregation and analysis also apply to private corporations. As recent disclosures have shown, the symbiosis between corporate and governmental data collection can be murky. The Commission recognizes that businesses also have an obligation to protect human rights.

Generally speaking, national legislation has not kept pace with Internet technology innovations. Existing legal frameworks do not always address the expanded surveillance capabilities that modern technology can allow.[42] For example, many states do not have adequate legal provisions on the collection, disclosure and use of metadata, on malicious computer hacking or on regulating access to bulk databases of personal information by their authorities. Some countries are now tackling this issue by distinguishing in law between the equivalent of communications data, widely used by all law enforcement organizations, and the deeper metadata such as the full browsing history of an individual that should require the same high level of authorization as would access to the content of an individual's communications.

Very few nations have adequate independent accountability mechanisms and judicial oversight, which are necessary to keep state power in check. Some states, governments and militaries are even known to actively stockpile vulnerabilities, develop malware or subvert security standards, which can then be used to conduct targeted or mass surveillance. Most of this activity was conducted in secrecy and left largely unregulated, posing threats not only to the ongoing security and stability of the Internet, but to freedom and democracy. Today, it is increasingly recognized by human rights experts and leading technologists that any attempt to weaken the security of the systems on which the Internet depends threatens every nation's interests.[43]

Inadequate legal provisions increase the risk of an individual's rights being violated. They can also have disproportionately negative implications for certain groups of individuals — such as members of political, religious, ethnic or social groups — who may be more likely to be placed under surveillance by the state based on aspects of their identity. This can lead to self-censorship or the violation of confidentiality for lawyers or journalists. Furthermore, government mass surveillance can impose considerable costs on business. After the revelation of US surveillance practices, there was a loss of trust in US cloud and

network equipment providers, major social media websites, search engines and email providers, ultimately impacting the profit margins of these companies.

There is a tension between the nature of the Internet, as a global, unified network and national, sovereign approaches to the governance of privacy, freedom of speech, protection from hate speech and personal data protection. Uncertainties created by the existence of legal regimes that are vastly different from one another can hinder innovation and have negative implications for the enjoyment of human rights. The IETF has recently moved to help combat some of the threats posed by government surveillance, the inconsistent regulatory frameworks in place to deal with new problems posed by the Internet, and the incompatibility of different jurisdictions' laws intended to address those problems.[44] Its statement argues that pervasive monitoring is an attack on individual privacy and technical steps need to be taken wherever possible to prevent such surveillance. Other organizations also have advanced a variety of principles intended to begin addressing the existing gaps in legislation. A recent example is the 2013 International Principles on the Application of Human Rights to Communications Surveillance, developed at the initiative of civil society.[45] These principles serve as an important reference regarding how international human rights law should apply in the digital environment in the context of communications surveillance. States are called to comply with the following principles: legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, safeguards against illegitimate access and the right to effective remedy. It is worth noting that this issue is not new. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted in 1980 and revised in 2013, state that exceptions to its principles, including those relating to national sovereignty, national security and public policy (*ordre public*), should be as few as possible, and should always be made known to the public.[46]

States are obliged to protect and promote rights to privacy and freedom of expression. Even if they are not absolute rights, limitations to these rights, even those based on national security concerns, must be prescribed by law, guaranteeing that exceptions are both necessary and proportionate. Any interference with the right to privacy should not be arbitrary or unlawful, bearing in mind what is reasonable to the pursuit of legitimate aims. It is also important that governments guarantee the same human rights protection to all individuals within or beyond their borders as they do their own citizens.

Recommendation

Interception of communications and collection and analysis of data over the Internet by law enforcement and government intelligence agencies should be for legitimate purposes, openly specified in advance, authorized by law and requiring the application of the principles of necessity and proportionality. Purposes such as gaining domestic political advantage, industrial espionage or repression are not legitimate.

Recommendation

Laws concerning data collection and surveillance should be publicly accessible, clear, precise, comprehensive and non-discriminatory, openly arrived at and transparent to individuals and businesses. Their application should be overseen by a competent judicial authority, and robust independent mechanisms should be in place to ensure accountability and respect for rights. Suspected abuses of the right to privacy should be amenable to independent judicial investigation with access to an effective remedy provided to individuals whose right to privacy has been violated by unlawful or arbitrary surveillance.

Encryption and Anonymity

The massive growth in transmission of both human and machine data brought about by the Internet, coupled with online censorship and mass and targeted surveillance, offers governments, corporations and criminals new opportunities to interfere with privacy rights. Encryption and anonymity-enabling technologies are often used to improve the digital security and privacy of individuals and businesses, empowering them to make secure financial transactions online or to read, browse or share ideas and opinions without interference. In more repressive regimes, where states impose censorship, encryption and anonymity-granting technologies are essential for activism, political dissent, education and democracy, empowering individuals to circumvent barriers, access information, organize collectively and share ideas without the interference of authorities. Weakening encryption standards or allowing governments access to these kinds of secured communications can endanger those who rely on encyryption technology to exercise their right to free speech and privacy. From a national security perspective, weakening encryption can also make governments more vulnerable to cyber espionage and foreign surveillance, as the state increasingly relies upon the Internet to carry out its day-to-day activities.

Nevertheless, law enforcement and intelligence agencies have complained that these technologies reduce their capacity to conduct investigations and prosecute criminal activity. Harassment, cyber bullying, hate speech and Internet trolling can take place behind a mask of anonymity. Knowing the identity of the individual behind the screen can help law enforcement agencies find and prosecute those who commit these acts. Encryption has also been identified as a technology that inhibits not only the investigation and prosecution of criminals and terrorists, but also the prevention of everyday cyber security threats. For example, the ability to monitor information sent across the network and stored online is essential for filtering spam and stopping the proliferation of illegal content, including child pornography, online. However, not all of the information used by law enforcement agencies is encrypted and inaccessible. As the 2016 Harvard report on the "going dark" debate on encryption and law enforcement found:

> Metadata is not encrypted, and the vast majority is likely to remain so. This is data that needs to stay unencrypted in order for the systems to operate: location data from cell phones and other devices, telephone calling records, header information in e-mail, and so on. This information provides an enormous amount of surveillance data that was unavailable before these systems became widespread.[47]

Encryption and anonymity have always been politically charged topics. In many contexts, states have placed a number of restrictions on opportunities for encryption and anonymous communication. Identification is required when a user purchases a SIM card for a mobile telephone, and it is sometimes required when users visit a major website or to register for social media websites or blogs. Anonymity online will be challenged further as future Internet users connect via mobile phones and the IoT vastly expands the number of identification and authorization technologies. Some law enforcement agencies have also demanded that companies hand over keys to encrypted data believed to contain evidence relevant to criminal and counter terrorist investigations. Where access to data is legally warranted, companies should provide data where it is practicable or technically feasible to do so, and where doing so does not unreasonably endanger the security of others' data.

Anonymity-granting technologies and end-to-end encryption provide the security and privacy necessary for exercising fundamental human rights online and for individuals, businesses and governments to engage activities that support economic growth and social progress. Increasingly, these technologies are essential enablers of freedom of expression, freedom of assembly and association, privacy and the right to life. Encryption technology is also the bedrock for the global digital economy and is used to secure online payment systems, and for sensitive interactions with government such as providing tax information. Without encryption, these and other vital functions using the Internet would not be possible. The legal

default for all states should be to protect encryption and anonymity-granting technologies. Any infringements on the technology must be prescribed by law and in line with the principles of necessity and proportionality.

Defining what is reasonable and practical and proportionate in all circumstances will never be easy. While certain restrictions on anonymity and encryption are important and can be justified for specific law enforcement activities, it is vital that the cost of such restrictions is viewed alongside the benefits that anonymity and encryption bring. Law enforcement and companies, the technical community and civil society must all engage constructively in the debate about where appropriate boundaries lie.

Recommendation

Consistent with the International Covenant on Civil and Political Rights, no one should be subject to arbitrary interference with their privacy, including privacy of their communications, regardless of the technology used. Governments should not compromise or require third parties to weaken or compromise encryption standards, for example, through hidden "backdoors" into the technology as such efforts would weaken the overall security of digital data flows and transactions. The Internet technical community should be encouraged to incorporate privacy-enhancing solutions into the standards and protocols of the Internet, including the use of encryption of data in transit and at rest. Access to data should be legally warranted only where providing access does not unreasonably endanger the security of others' data. Laws have to be updated and norms need to be established so that Internet companies, the technical community, law enforcement and civil society can engage cooperatively in seeking solutions as to how public security can be enhanced overall by new technologies, while the privatization of law enforcement, responsibility of human rights and governance is avoided.

Censorship

Innovations in technology have given states and corporations the technical capability, if they so choose, to conduct widespread filtering and censorship of online activity. A number of filtering technologies exist that allow states to scan communications across the Internet and identify certain words, voices or phrases that can be used to filter Internet activity. These technologies and methods go beyond gaining simple knowledge about the sites that an individual visits and can instead be used to analyze and block access to the content of websites.

The discussion of censorship has been contentious for policy makers as well as for free speech advocates. The Internet is an incredibly powerful communication platform that can foster cohesion among geographically distributed and diverse groups of people, and give individuals access to a vast amount of knowledge that can be used to improve their quality of life. However, this shift in communicative power has led to increased efforts by governments to restrict the flow of information and control content on moral, cultural, religious or political grounds. While all countries have some technical capacity to censor content, it can be hard to tell to what extent any particular government actively engages in blocking materials online. It is important to note that corporations also block and censor content for a variety of purposes. Censorship by private actors is discussed further in the next section.

Some states have developed and used very sophisticated censorship tools that allow them to censor on the grounds of political dissent or religious beliefs.[§] When combined with surveillance technology, these tools are especially insidious, as they can be used to track down, persecute and imprison activists, educators, artists, journalists or other individuals based on their identity or beliefs, ultimately having chilling effects on freedom of expression, freedom of assembly, privacy and democracy.

[§] See, for example, the Citizen Lab's Open Net Initiative at https://opennet.net/.

PAKISTAN'S YOUTUBE BLOCK

In 2008, the Pakistani government censored YouTube by ordering the redirection of Internet traffic away from the website. However, when the routing information was not contained within the local network, many people outside of Pakistan were directed to the network block. While this example reveals a number of implications for the reliability of the Internet, it also shows how poorly informed or badly executed attempts to achieve social ends can have on freedom of expression. In 2012, YouTube was blocked again after an inflammatory video sparked a number of protests across the country and the Muslim world. The ban on YouTube lasted three years, until January 2016, when YouTube agreed to launch a local version of its site in the country. Under the agreement, the Pakistan Telecommunications Authority can ask YouTube to remove any material it deems offensive. Pakistan is not the only country that maintains a localized site: there are currently more than 85 country-specific YouTube home pages around the world. Most of the time, it is unclear to what extent the government is demanding the removal of content and for what purposes. Although many companies publish transparency reports, there is no transparency around the kinds of requests governments are making and what the companies are choosing to comply with.

Furthermore, many censorship tactics block content by exploiting weaknesses in the existing Internet infrastructure and standards. These kinds of tactics can have negative implications for the overall reliability of the Internet that extend far beyond the borders of the country attempting to impose censorship.

Governments should promote and protect freedom of expression and take steps to encourage the free flow of information online. However, it is important to recognize that some Internet content can be illegal. While ensuring consistency with international human rights standards, governments should make clear to the public what kinds of content they intend to restrict online. Any restrictions to online speech and content must be prescribed by law, pursuant to a legitimate aim, and necessary to achieve that aim. Censorship for political or economic advantage, or discrimination against any religious or other identifiable group of people is not legitimate. Consistent with the UN Joint Declaration on Freedom of Expression and Responses to Conflict Situations, shutting down entire parts of communications systems to block objectionable content can never be justified under human rights law.

Recommendation

Private actors should not become the enforcement arm of governments. Any special or secret agreements between governments and private actors to restrict or limit access to Internet content, or to limit access to communication should be made transparent. Illegal public-private cooperation should be terminated. Private companies should publish transparency reports that reveal the amount of content being restricted or blocked in response to requests by governments, for what purposes and by what means. Governments must allow companies to publish aggregate information about what they have requested and how the company responded. Civil society plays an important watchdog role. In addition to the volume of requests made, the terms under which companies must comply with government requests must be made open and the rationale for removal must be made transparent.

Extraterritoriality

Because of the transnational nature of the Internet, the issues surrounding the impact, both positive and negative, of intelligence and law enforcement activity on human rights do not stop at state borders. Liberal democratic states afford some protections to those in their jurisdiction against unwarranted surveillance, but do not have authority beyond their borders. Some states claim extraterritorial application of their domestic law over Internet companies providing services in their jurisdiction, but when based overseas such companies can then find themselves subject to a clash of laws absent bilateral legislative agreements. This problem is exacerbated for two reasons. First is that many of the key Internet infrastructure and connection points are located in a limited number of jurisdictions. The second reason is that data is routed on the principle of efficiency. Thus, individuals often do not choose or even know where their data is housed. It is even more certain that individuals do not choose where their packets are sent by the network before they reach their final destination. These two factors mean that an individual's data often fall subject to foreign laws that may have less stringent privacy or security protections than the individual's home jurisdiction. This issue applies as well to personal data held by private-sector companies that, for commercial reasons, wish to store or process it overseas.

In 2013, leaked government documents appeared to reveal that the US government was acquiring user data from US cloud providers and Internet companies. This caused an outcry from domestic and international communities: profits dropped as customers around the world lost confidence in these companies.[48] In addition to demands for new data privacy standards, many countries are now requiring companies to store data locally — in an attempt to shield it from international surveillance. According to Matthias Bauer, Martina F. Ferracane and Erik van der Marel in GCIG Paper No. 30, data localization can result in efficiency losses that undermine economic productivity and growth.[49] Furthermore, data localization is not an effective way to address the crux of the surveillance problem: malware can be installed on servers to collect, interpret and redirect traffic, and data can be intercepted while in transit through other jurisdictions. Data localization also increases the opportunity for states to conduct surveillance nationally. It is important to note that the problem of data localization goes beyond the scope of surveillance — many countries use localization requirements to conduct censorship and silence dissent, or in an attempt to protect sensitive data from leaving the country.

International sharing agreements also pose a new issue for privacy and the protection of personal data. Governments may be tempted to use the ambiguity created by the borderless nature of the Internet to spy on their own citizens abroad, or to arrange with their sharing-agreement correspondents to collect information in their sovereign space. Such agreements must not be used to gather information about individuals that would not be authorized by domestic law in the participating states. Sharing agreements can be important tools for dismantling terrorist or international criminal networks. However, if they are used to circumvent national laws on data collection or protecting privacy, sharing agreements pose a serious threat to human rights and democracy.

Improving Export Controls for Surveillance Technologies

Some aspects of the market in ready made or "click and play" surveillance technologies are largely unregulated. This is remarkable for a retail market that was estimated in 2011 to have a value of around $5 billion a year. In particular, the unregulated market for exfiltration technologies has serious security and human rights implications. Civil society organizations and investigative journalists have demonstrated how these systems are actively marketed and sold to governmental actors with dubious human rights records, who then use them to spy upon journalists, human rights activists or opposition figures. After one of the sellers of these surveillance technologies was hacked, it claimed that its tools could now freely be used by criminals and terrorists.

Controlling the abuse of surveillance, lawful-intercept and other targeted digital-attack technologies needs to be managed by a multi-pronged approach. To date, the primary focus of this debate has revolved around the 2013 agreement among 41 states — known as the

Recommendation

International data-sharing agreements between governments should not be used to circumvent the national laws of a country and should respect human rights. Intelligence agencies should be subject to democratic and judicial oversight.

Recommendation

A multi-pronged approach is needed to address the ongoing issues related to export control and dual-use technologies. In addition to bringing in human rights considerations, and improving the existing definition of intrusion software in the Wassenaar Arrangement, more recognition should be accorded public research efforts, and "smart" regulatory approaches are needed to provide industry with guidance on what are acceptable limits in their research and development of security products.

Wassenaar Arrangement — to accept proposals to extend the list of items accepted as being subject to export controls to include "intrusion software" and "IP network communications surveillance systems," as well as related software, systems, equipment and components. This revision was heavily criticized by the security community and industry, resulting in renewed efforts to renegotiate the language. Unfortunately, governments' focus on one remedial instrument has obscured other approaches, such as the use of legal remedies and the importance of public research conducted by organizations like the Citizen Lab.[50] In addition, pressures could be brought to bear on companies themselves, requiring them to be more transparent and accountable about the abuse of their products and services.

The Protection of Children Online

One of every three Internet users in the world is a child.[51] The Internet is becoming the main medium through which children collaborate, share, learn and play. Research conducted for the GCIG has demonstrated that the Internet can help transform a child's learning opportunities by increasing their access to knowledge and online resources at new and unprecedented rates,[52] and can provide new opportunities for civic engagement or individual expression through content creation and social media.[53]

However, protecting children online, as in the physical world, requires special consideration. A two-pronged approach is most effective. As digital natives, children are often far more well-versed in digital technologies than their parents, teachers or legal guardians. But they are still children, and are often not aware of the potential harm that could occur to them while online. One pillar of online safety for children is child empowerment. Whether through government educational programs, schools, community programs or camps, children need to be taught how to protect themselves while using the Internet.

The second pillar for keeping children safe online is child protection. Law enforcement plays a key role in tracking, arresting and prosecuting criminals who target children. Law enforcement's work is being both complicated and enhanced by new technologies. The Onion Router (Tor), for example, is a boon for those who would hurt children, as it provides for anonymous web browsing, which can allow an offender to view and upload child abuse content with less chance of being caught by the police. Technological advances can also help law enforcement identify perpetrators and victims. For example, the ability to ascertain fingerprints from digital photos or the use of hashes all assist law enforcement in finding perpetrators and victims, so they can remove illegal content.

Enforcement is not confined to law enforcement alone. Private companies can also help to protect children online by actively taking down illegal content from their services. Parents, too, need to be watchful of what their children are doing online, and recognize that many youth spend an inordinate amount of time interacting with others via digital technologies.

The Responsibilities of the Private Sector

Our online lives, to an ever-greater extent, are becoming reliant on private sector companies in one of three roles: as providers of Internet access; as Internet-based providers of content or other digital goods; or as providers of traditional goods and services, as online retailers or by offering augmented banking, insurance or other services. In all of these roles, corporate actors of all sizes are able to exert greater influence over our lives and fundamental human rights.

Corporations regularly store, manipulate and analyze our data as we use their networks and infrastructure to find or create content, send emails or messages to our friends and family, engage in commercial transactions, or to share and store content. Private sector actors are also increasingly "digital gatekeepers" who control the flow of information across the network. As gatekeepers, they have the ability to decide whether to deliver content or to take it down. They determine how fast or slowly we send and receive data. They also have the power to suspend or delete user accounts. Companies that play these roles are known as Internet intermediaries. The Association for Progressive Communication has identified two kinds of Internet intermediaries: "conduits," which provide Internet access or transmission services; and "hosts," which provide content services such as online platforms or storage services.[54]

As the commercial Internet emerged, the number of users grew exponentially, along with the amount and type of Internet content being exchanged. This explosion has provided new kinds of business opportunities for intermediaries by indexing, organizing, using and selling the data and information about its users. Coupled with the increasing digitization of everything, the behaviour of private sector actors is introducing new and significant challenges for human rights online.

Commercial Data Gathering, Processing and Use

Access to data is increasingly valuable, driving much of the global information economy. Many companies operating on the Internet are building businesses on their ability to use and sell the data they gather. Today, the business models of many online companies are based on advertising, where user data is collected and stored in exchange for providing a "free" service to their users, and then sold directly or indirectly to third parties. Data collected from customers are often used for purposes not explicitly revealed to those who provide the data, and used without their permission.

Creative approaches to aggregating and manipulating data are fuelling analytics to the benefit of innovation (i.e., data-driven innovation). Open data — that is, machine-readable information, particularly government data made available to others — has the potential to empower citizens, improve government transparency and improve the delivery of public services.[55] It can become an instrument for breaking down information gaps across industries, allowing companies to share benchmarks and spread best practices that raise productivity. Real-time data combined with analytics can provide unique insight into some of the world's most serious problems, including disease outbreaks, food shortages and price volatility, global financial crises or human rights violations. However, data sharing raises important concerns about respect for users' privacy and security, as well as about who owns the data and under what conditions. These concerns only increase with the growth of the IoT.

Commercial use of personal data usually involves its collection and packaging for commercial or marketing purposes. A thriving market has emerged in the collection, aggregation and analysis of individuals' data. Firms accrue tremendous benefits from analyzing personal and communications information. Companies use big data analytics to glean detailed customer insights that enable them to tailor their products and strategies for micro-segments of the marketplace.[56] Data analysis can lead to better targeted advertising by companies, and can helpfully point users toward products they may be interested in. Companies such as YouTube and Amazon frequently analyze their users' viewing and shopping habits, making recommendations based on their previous interests and preferences. Similarly, real-time location data can be useful for improving commute times. For example, applications such as Waze or Google Maps provide traffic updates and optimize travel routes based on real-time location data. While there is value for individuals in the aggregation of personal information, it is essential that individuals are informed of, and given the option to consent to, the various uses of their data.

Internet users — the primary source of communications data — may be unaware that they are producing data (or causing data about themselves to be produced), either directly or as the basis for inference, that could be valuable to others. They may also not be aware of what their data is being used for or who is using it. When users' personal information is sold to third parties, it becomes significantly more difficult to track, making it hard for individuals to know who has access to their information, how it is being used and for how long. Although this information is sometimes made available in terms of service agreements, people routinely consent to them without reading the full agreements or understanding how companies are using or misusing their information. Often, terms of service agreements are unavoidable in the context of what a user wants to do, and users have little to no ability to negotiate the contracts themselves. In addition, there are not any real options to accepting the terms dictated by corporations: certain dominant Internet service providers — such as search engines, email or social media — have become an essential part of society. Opting out of these agreements can amount to opting out of the networked economy and digital public sphere.

Today, some companies surpass governments in their capacity to collect, store, integrate analyze and make use of personal and transactional data. These companies are increasingly attractive targets for cyber infiltration by criminals or pranksters, and

GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

Collection Limitation Principle

1. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

2. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

3. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

4. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
   a) with the consent of the data subject; or
   b) by the authority of law.

Security Safeguards Principle

5. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

6. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

7. An individual should have the right:
   a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
   c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
   d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

8. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Source: "OECD Guidelines on the Protection of Privacy and Transborder Flows of Person Data."[57]

susceptible to efforts to jeopardize the confidentiality, availability and integrity of these large data pools. To maintain their users' confidence, companies have to demonstrate a high level of respect for, and protection of, the security and privacy of their information holdings. At the same time, companies must exhibit accountability to both governments and customers by demonstrating good stewardship in responding to lawful government requests for access to their users' data. They also must contend with increasing numbers of requests for access to data from foreign law enforcement agencies, due to the transborder nature of many activities taking place on the Internet. These responsibilities can and do put companies in unfamiliar and difficult situations where they need to make judgment calls on how to respond appropriately to competing demands. The Commission supports the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as a source of inspiration for managing these difficult situations.

We must reverse the potential for eroding trust in the Internet brought about by the non-transparent market in collecting, centralizing, integrating, analyzing and exploiting enormous quantities of private information about individuals. There are growing calls for regulators, or for the industry itself, to establish standards for transparency and accountability mechanisms to increase confidence in the marketplace. For example, the Digital Equilibrium Project — which brings together stakeholders from privacy, technology commercial, law enforcement and national security communities — has suggested a "transactional model" for privacy, which enables users to understand, set and change the parameters under which their data will be stored, used and shared.[58]

Corporations as Digital Gatekeepers

Algorithms and Access to Information

Our online world is increasingly being structured by "algorithmic decision making," where companies and other actors hosting big data sets use complex statistical formulas — algorithms — to analyze their data to identify patterns and make future predictions, sometimes resulting in surprisingly accurate profiles of demographic groups down to the individual level. Search engines, banks, insurance providers and credit rating agencies are collecting information about individuals and converting it into ratings, scores and risk calculations, which have serious implications for our lives. The cross-platform nature of this collection can create a very detailed profile of an individual: a bad credit score can cost someone a mortgage, and a health risk calculation could increase the costs of one's health insurance or make them ineligible for

Recommendation

Individual users of paid or so-called "free services" provided on the Internet should know about and have some choice over the full range of ways in which their data will be deployed for commercial purposes. They should not be excluded from the use of software or services customary for participation in the information age, and should be offered the option of purchasing the service without having to agree to give the provider access to their personal information. Terms of use agreements should be written in a clear and accessible manner and should not be subject to change without the user's consent. Businesses should demonstrate accountability and provide redress in the case of a security breach or a breach of contract.

Recommendation

To assure the public that their data is being appropriately protected, states that do not already have comprehensive personal data protection legislation and a privacy enforcement authority with legal enforcement powers should take steps to create such regimes.

HOW ALGORITHMS CAN INFLUENCE HUMAN BEHAVIOUR

In 2012, Facebook conducted a week-long experiment that randomly selected approximately 700,000 users and exposed them to different types of emotional content. One group was exposed to positive content and the other to negative content. However, no information was given to users regarding the experiment. In fact, many did not even know they were participating. The study found that "[f]or people who had positive content reduced in their News Feed, a larger percentage of words in people's status updates were negative and a smaller percentage were positive. When negativity was reduced, the opposite pattern occurred. These results suggest that the emotions expressed by friends, via online social networks, influence our own moods, constituting, to our knowledge, the first experimental evidence for massive-scale emotional contagion via social networks."[59] Although this was just an experiment, it demonstrates the real power of large platforms to influence human behaviour. Search engines and other providers can modify our search results for different commercial, political or regulatory goals. However, it is unclear how these algorithmic decisions are made.

certain kinds of coverage. At the same time, these algorithms determine what a user sees: companies use algorithms to deliver recommendations based on shopping or viewing habits, and news agencies, social media and search engines use algorithms to deliver content that a user might like. Most of these algorithms are proprietary — leaving them immune from public scrutiny, transparency and accountability. This can have chilling effects on individual rights and democracy, by impacting human behaviour and opinion, and by limiting our ability to access the full range of content available to us online.

The impact of algorithms on people's lives is becoming more and more significant. The code that operates and governs the digital economy, access to information and other online activities is increasingly used to make decisions for us and about us. Algorithms written by corporations that operate online can decide what content receives attention and what gets ignored or censored. Algorithms are not necessarily neutral: they incorporate built-in values and serve business models that can lead to unintended biases, discrimination or economic harm. While many people are familiar with the role of algorithms in online searches or the curation of social media timelines, their role is expanding into areas such as hiring and finance. Employers, for example, can now access not only the type of information contained in traditional resumes, but also personal and reputational information regarding job seekers and employees. These are data-driven insights that could be used to reduce job discrimination or to introduce new forms of it.[60] The increasing use of algorithms across society comes with considerable risks that the underlying data and algorithms could lead to unexpected false results, in particular when the algorithms are used for automated decision making.

Data-driven innovation and the IoT are increasing the number of automated decisions based on algorithmic calculations, which creates more than just digital security concerns; it produces ethical and legal ones as well. To ensure that the public interest and individual rights are safeguarded, some oversight and accountability are needed. The creation of liability frameworks is one avenue for policy makers to consider as they begin addressing security risks.[61]

In particular, given the social and economic costs to third parties and individuals, further thinking on the attribution of responsibility for inappropriate decisions and the attribution of liability between decision makers, data and algorithm providers is necessary. This also calls for a careful examination of the appropriateness of fully automated decision making and the consideration of transparency requirements and human intervention in areas where the potential harm of such decisions may be

significant (for example, harm to the life and well-being of individuals, or the denial of economic or social rights).

Despite their increasing impact on societies, algorithms remain highly opaque. That makes it difficult for outsiders to understand the rationale behind algorithm-driven outcomes and to assess algorithms' (unintended or collateral) effects. Understanding the purpose and outcome of algorithms will be increasingly important for enforcement of competition and consumer protection policies. Government agencies are beginning to investigate the implications of requiring algorithmic transparency. However, asking corporations to reveal the complete algorithms on which the health of their business rests is probably unrealizable. Algorithms benefit from intellectual property rights protection, and in many cases underlie the basic business models of large companies.

Furthermore, a full algorithmic transparency requirement would not necessarily always be a good idea, even from a public perspective. Drafting and implementing regulation would involve trade-offs, consideration of special cases, application of a variety of policy considerations beyond privacy, and the potential for creating whole new sets of unintended consequences. For example, although the functional core of Google's algorithm has been known for years, certain aspects of the algorithm are held as trade secrets. Some of the secret elements are designed to thwart search engine optimizers, which are services that aim to boost a site's rank in search results by attempting to understand a search engine's methods and manipulate them to distort the results in a client's favour. The effectiveness of those aspects of the algorithm depends on their remaining secret. Some critics of the idea that Google should be required to disclose its full algorithm therefore contend that the result of full algorithmic transparency would not only be bad for Google, but for all users of their services. The optimizers would be granted complete knowledge of how the algorithm works, and with that information in their hands, Google's search results would soon become distorted and unreliable.

The debate about algorithmic transparency, like the debates around intellectual property protection, are unlikely to be resolved anytime soon, given that strong views are held on both sides. Although algorithmic transparency can be viewed as a good thing because it would enable oversight to protect the public interest and individual rights, and even though that transparency would increase knowledge diffusion and is viewed by some to be positive since it promotes innovation, there are special cases in which society may be better off if proprietary algorithms remain out of public view. Furthermore, although it may seem intuitively true that algorithmic transparency would promote competition (for example, by discouraging search engines from favouring their own subsidiary businesses in search results), the example above shows that transparency is just as capable of harming competition as non-transparency.

One possibility is to make algorithmic verifiability rather than full algorithmic transparency an element of oversight in the digital economy. This algorithmic verifiability would require companies to disclose information allowing the *effect* of their algorithms to be independently assessed, but not the actual code driving the algorithm. Without an understanding of the impact of algorithms, competition and antitrust investigations, as well as actions to address liability, can become virtually impossible. Nonetheless, the possibility of unintended consequences and special cases — even with respect to this more limited type of algorithmic disclosure — suggests that the costs and benefits of algorithmic verifiability should be widely studied before any regulatory action is recommended, and that this should be done in an inclusive manner, involving stakeholders from across the spectrum of policy domains that could be affected.

Recommendation

Because algorithms are set to have such an all-pervasive effect on society, governments, private sector representatives, civil society and technologists need to come to together to study their effects.

Freedom of Expression and Intermediary Liability

Companies have increasingly become the arbiters of freedom of expression. Through their ability to impose the takedown of private content, companies are increasingly navigating difficult social problems, ranging from hate speech, harassment and cyberbullying to revenge pornography or child pornography. Every day, content providers and intermediaries must determine whether to block content that engenders hatred or violence, and on whose authority. Although some kinds of content, such as child pornography, are reprehensible in virtually all societies, other kinds of content may be legal in one society and illegal in another. Questions of culturally determined values and morality pose even more difficult problems. The line between what to block and what to maintain is not easy to draw, as Emily Taylor notes in GCIG Paper No. 24, "decisions are difficult, nuanced and different cultures have varying tolerance levels."[62]

As the transnational nature of the Internet forces private companies to play a growing role as policy makers in spaces where governance was traditionally carried out by the state, there are increasingly contentious battles taking place at the intersection of intermediary liability, personal privacy and access to information. In 2014, a Spanish man brought a case to the Court of Justice of the European Union, complaining that Google's search results indexed news stories that contained personal information about his past financial difficulties. As a result of this complaint, the Court of Justice ruled that personal data should be removed from search results on a person's name when this information is outdated, inaccurate, inadequate, irrelevant or devoid of purpose, and when there is no public interest. Ultimately, this caused a wave of requests made by citizens concerned with protecting their personal privacy.

However, this decision was widely criticized on the basis of its potential to create a number of problems for freedom of expression and human rights.[63] The delisted search results are not accessible to any user in the European Union. Questions then arise about whether this is the appropriate way to implement the court ruling, including whether or not the removal of search results should be imposed in all territories served by Google. One of the biggest flaws of the ruling is that it places a commercial company in the uncomfortable position where they are required to determine the appropriate balance between the right to privacy of a person versus the interest of the general public in accessing that information. While Google posts the number of requests it complies with, it does not provide any transparency in the reasoning for removing certain instances of searchable content and not others. Private companies — as opposed to courts and legislatures — are only accountable to their shareholders; they should not be the arbitrator on how to weigh fundamental rights and public interests.

Content intermediaries are evolving institutions. As a result, government policy makers are struggling to understand these new roles and to determine whether and how to legislate or regulate new behaviours in this nascent and fast-changing industry. The situation is further complicated by the transnational reach of these intermediaries. The concept of Internet intermediary liability has emerged as a way to regulate or require the takedown of harmful or illegal content. Intermediary liability can be applied in a variety of contexts, including: copyright infringements, digital piracy, trademark disputes, network management, spamming and phishing, cybercrime, defamation, hate speech, child pornography, censorship or privacy protection.[64]

Different governments have developed different models of liability. For some governments, intermediaries can be held liable for content because they directly contributed to an illegal activity or because they had the ability to control the content and derived some kind of financial benefit by not doing so. Other governments offer "safe harbours" to intermediaries, where they are not liable for user actions on their platforms as long as their own actions stay within the rules laid out in the safe harbour provision. Safe harbours are considered an important element in supporting the emergence of innovative services by providing intermediaries with enough legal clarity to conduct a wide range of activities

MANILA PRINCIPLES ON INTERMEDIARY LIABILITY

Introduction

All communication over the Internet is facilitated by intermediaries such as Internet access providers, social networks, and search engines. The policies governing the legal liability of intermediaries for the content of these communications have an impact on users' rights, including freedom of expression, freedom of association and the right to privacy.

With the aim of protecting freedom of expression and creating an enabling environment for innovation, which balances the needs of governments and other stakeholders, civil society groups from around the world have come together to propose this framework of baseline safeguards and best practices. These are based on international human rights instruments and other international legal frameworks.

Principles:

1. Intermediaries should be shielded from liability for third-party content.
2. Content must not be required to be restricted without an order by a judicial authority.
3. Requests for restrictions of content must be clear, unambiguous, and follow due process.
4. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.
5. Laws and content restriction policies and practices must respect due process.
6. Transparency and accountability must be built into laws and content restriction policies and practices.

Source: https://www.manilaprinciples.org/ .

without the fear of potential litigation. However, there are also concerns that overly broad safe harbours are sometimes in contention with incentives to uphold human rights online.[65] Civil society and human rights activists have begun to propose the adoption of principles on intermediary liability, to promote freedom of expression and enable innovation. The Manila Principles on Intermediary Liability outline a number of legal principles that the Commission fully supports, including: shielding intermediaries from liability for third-party content; the requirement of judicial authority for content takedowns; necessity and proportionality; clarity and due process; and transparency and accountability.

The Commission also believes that actors in the digital ecosystem — whether technology companies or intermediaries such as content hosts or ISPs — should not be required to perform the functions of law enforcement, except as required by appropriate judicial order.

Recommendation

Legally required takedown of content should happen at the source of the content — or where it is being hosted. Data aggregators and social media websites must be responsible for the takedown of unlawful content that is hosted by them. Any takedowns should be subject to the legal principles of openness, conflict of interest, transparency and appeal. Network operators and Internet intermediaries should not be held liable for the use of their infrastructure or services for illegal purposes. At the same time, when presented with legitimate warrants, private companies should cooperate with law enforcement agencies.

Infrastructure and Service Intermediaries, Freedom of Expression and Network Neutrality

Thus far, this section has spoken to the role of content intermediaries in relation to law enforcement, particularly with regard to human rights. However, infrastructure and service intermediaries — or companies that handle the transmission of data — are also important private sector actors that may influence and, in some cases, govern how we access information online. Like content intermediaries, infrastructure and service intermediaries can block content. Notably, these actors have different tools at their disposal. Instead of issuing takedown notices, infrastructure and services intermediaries can redirect traffic away from websites. While these actions do not remove content from its source, they can effectively remove the pathways that allow users to access it. In some countries, infrastructure and service intermediaries are used to block access to certain websites — including social media websites such as Twitter, Facebook or YouTube, or websites where pirated and copyright material is being hosted. Difficult questions have arisen, including what might be the justification for requiring a private entity to act in lieu of a law enforcement agency, and under what conditions.

Similarly, infrastructure and service intermediaries can influence or determine the conditions under which content is made available to users. An active debate, generally known as the network neutrality issue, has emerged over what types of control are acceptable and under what circumstances.[66] Network neutrality is the principle that Internet traffic should be treated equally and that network operators should be prohibited from prioritizing, throttling or blocking particular types of traffic that flow across their network. The Commission supports the idea that Internet traffic should be treated equally, without discrimination, restriction or interference, independent of the sender, receiver, type, content, device, service or application. This principle does not rule out so-called "specialized services" such as hospital-to-hospital communications that require higher speeds or routine traffic engineering and management practices that ISPs regularly engage in.

Some network operators argue that traffic management techniques can be used to improve the overall efficiency of the network. For example, VoIP (voice over Internet Protocol) calls or other streaming services may be given priority over email content, as delays make a noticeable difference in streaming video as opposed to sending and receiving emails. However, there are serious concerns that network operators may go beyond what is necessary to ensure that data is flowing smoothly and efficiently across their networks. For example, given the dominance of the large Internet content providers and a very few service providers, there has been concern that some network operators may be using traffic management techniques to benefit their own or their partners' services or for other types of commercial gain, or to help achieve political goals. For example, some media coverage has demonstrated the governance role that can be played by network operators in curbing online piracy, by throttling a user's home Internet when they are uploading and downloading large amounts of data.[67]

Recommendation

In order to keep the Internet open and to foster innovation and competition through the digital ecosystem, regulators should demand transparency and prohibit arbitrary discrimination by the main gatekeepers across the value chain. This would include blocking legal content or applications, throttling network speed or anti-competitive behaviour to advantage the gatekeeper's preferred services. Consistent with good regulatory practice, a technologically neutral approach should be sought.

Safeguarding the Stability and Resiliency of the Internet's Core Infrastructure

When most people think about the Internet, what usually comes to mind is the content it makes available or the tools that enhance their social, economic, intellectual and political lives. Beneath the surface level of content, of course, is a globally distributed ecosystem of logical and physical infrastructure that keeps the Internet operational and creates the conditions for digital innovation and the free flow of information. In the twenty-first century, trust in digital markets and, to an increasing extent, the public sphere, political systems and industrial control systems requires trust in this underlying technical infrastructure. This infrastructure is not static but continuously evolving and shaped by the values of its designers. The success and growth of the Internet can convey a sense that this underlying technological ecosystem is stable, secure and resilient, but these qualities cannot be taken for granted.

Several global developments are challenging rather than strengthening the stability and universal reach of the Internet. Some of these problems are technical, such as new security challenges arising from the IoT. Some are economic, such as the private industry movement toward proprietary and walled services. Some are political, such as governments placing restrictions on where private companies store customer data or attempting to impose other alterations to Internet infrastructure with the goal of achieving unrelated policy objectives. In some cases, political objectives and ideologies such as cyber sovereignty, where governments seek to exercise control over the Internet infrastructure within their own borders, conflict with how the topology and global infrastructure of the Internet actually works in practice. The advocacy of multilateral or top-down governance approaches versus multi-stakeholder approaches can also be seen as a conflict between a

Westphalian or "bordered" view of the Internet and a topological infrastructure view.

The Commission believes that it is necessary to preserve the core transnational infrastructure of the Internet to support the global digital economy and the free global flow of information. The Commission calls upon private industry and governments to reject approaches that tamper with the Internet's core global infrastructure for political advantage; instead, they should promote the technological conditions that enhance the stability and resiliency of the universal and open Internet infrastructure so essential for continued growth in the digital economy.

The Public Interest in the Stability and Resiliency of Internet Infrastructure

Much of the global attention on Internet governance focuses on content-centric issues, including concerns about freedom of expression, intellectual property rights enforcement, data breaches and spam. Another set of governance concerns addresses usage issues such as the effects of Internet penetration on global trade and development. Often missing in these discussions is attention to the Internet infrastructure, rather than the content that traverses it, the applications that make it easy to use or the people that communicate over it.

The vast majority of the virtual and physical infrastructure of the Internet is invisible to those who use it, although it is becoming as important to society as natural resources. This infrastructure includes interconnection points, technical protocols, security architectures, intermediary platforms, wireless systems, radio frequency spectrum and satellite orbital slot allocations, undersea cables, human capacity, institutions, and names and numbers. Underlying all of these are other general-purpose critical infrastructures such as the power grid. This Internet infrastructure can be thought of as a shared global public resource, owned and operated primarily by the private sector. Trust in the markets, the public sphere and political systems that use the network requires trust in the digital infrastructures upon which all of these systems rely. The critical services of finance, trade, transportation, health care and industrial control applications for energy and water treatment are completely dependent upon the stability of this technical scaffolding. What is at stake is not just society's ability to communicate, but rather its ability to function day-to-day in all aspects of life. There will soon be 50 billion objects connected over the Internet. In the near future, it will be the daily reality of life that everything from wireless heart monitors to driverless cars will depend upon the Internet to function. In this context, the stability and resiliency of the Internet is essential, because it is the infrastructure on which all other infrastructures now depend.

Internet infrastructure is not static but evolutionary. History has shown that it is constantly evolving, and has so far managed to seamlessly accommodate diverse categories of platforms ranging from mobile systems to industrial sensor systems to digital health environments. This diversity will only increase in the future. The layered model of Internet protocols has helped enable this "organized chaos" of Internet adaptability. Stability and resiliency are essential for access and innovation, and they have coexisted and can continue to coexist despite technological disruption and change. This balance between stability and innovation is able to occur in part due to common technical standards designed to allow unanticipated innovation to occur.[64]

Internet infrastructure is not neutral. The design and implementation of infrastructure reflects particular social values and economic interests, and embeds the values held by its designers. The underlying values matter greatly. There is a reciprocal relationship between technical design and social forces. Technical decisions reflected in the design of the infrastructure shape what is possible to achieve through governance, and policies have a profound effect on the design, stability and resiliency of the underlying infrastructure. Stability in the face of ongoing innovation, change and disruption is not a given, but something that has to be continuously shaped by the design and administration of the system, which reside primarily in the technical community and the private sector.

Stability actually supports disruptive innovation. If the environment is not sufficiently predictable, innovation is impossible. So one needs sufficient stability for innovation to take place, but this should be established through means that do not inhibit innovation. Internet infrastructure has achieved an equilibrium between stability and disruptive innovation because of the reliance of certain design and administrative principles. These principles are well expressed by what the Internet Society (ISOC) describes as Internet invariants.[69] Specific technologies, protocols and transmission systems have continuously evolved, but arguably there have been some consistent technical norms shaping how the Internet is designed and administered, contributing to the resiliency and generativity of the Internet. These traditional (or historic) norms of Internet infrastructure include, among others:

- **global reach**: the potential of any end device to reach any other regardless of location;
- **general purpose**: the capacity to support a diversity of applications;
- **permissionless innovation**: in which anyone can introduce a new Internet application without a gatekeeper's consent;
- **accessibility** for anyone to consume or contribute content;
- **interoperability and mutual agreement**: to allow for connectivity among devices made by different manufacturers;
- **collaboration** among stakeholders (such as on standards);
- **reusable building blocks**: so that technologies can build upon existing innovations; and
- **no permanent favourites**: so that new entrepreneurs can introduce innovative new products that potentially become market leaders of the future.

Global reach and interoperability, in particular, are some of the design characteristics that have moved the Internet closer to universality and allowed for the transition from many non-interoperable networks to one interconnected Internet.[70] As Internet engineer Leslie Daigle has summarized in GCIG Paper No. 7, "A network that does not have these characteristics is a lesser thing than the Internet as it has been experienced to date."[71] While never perfectly implemented and always marked by tensions between conflicting interests and competing geopolitical values, these principles of infrastructure design and administration have enabled the Internet's growth and its architectural capacity for stability and resiliency in the midst of rapid innovation and creative destruction. Admittedly missing from the original design of the Internet are inherent security features such as confidentiality, integrity or authentication. For example, the DNS, in its original design, does not include cryptographic features to authenticate queries. Attempts to retrofit critical security features into various aspects of the Internet's design have been ongoing and continue today. Swift and widespread action now could ensure that security is built into the design of the IoT. The remainder of this section explains the trends that are eroding, rather than strengthening, the Internet's resiliency and highlights opportunities for policy makers and the private sector to cultivate the technological conditions that reflect the Internet's historic trajectory toward growth and innovation.

Pushing Back Against Trends That Destabilize Internet Infrastructure

Several global developments are poised to weaken rather than strengthen the resiliency of the Internet, which will have direct effects on the efficiency and cost of using the network.[72] These developments can be categorized as follows: Internet fragmentation; slow deployment of technologies such as Internet Protocol version 6 (IPv6) and Domain Name System Security Extensions (DNSSEC); policies that tamper with infrastructure arrangements in a way that could potentially compromise the Internet's stability; and the marketplace promotion of proprietary approaches. What these trends have in common are both a weakening of Internet infrastructure and a push toward the fragmentation of the Internet, rather than preserving the principles of universality and global reach.

Internet Fragmentation

Fragmentation is already a part of the Internet at several layers. At the infrastructure layer, a lack of basic Internet technologies, such as IXPs, limit users' access to the network and impede the quality of their service. At the logical layer, the incomplete transition from IPv4 to IPv6 creates problems of backward and forward compatibility, while at the content layer, the Internet is fragmented due to the censorship practices of repressive regimes. At the institutional layer, different legal regimes and regulatory environments fragment the norms and laws that govern cyberspace.[73]

Added to these already existing forms of fragmentation are a number of troubling trends that threaten to fragment the network even further.[74] One such trend is driven by private market forces. Many companies are now developing a number of propriety platforms that limit the traditional openness of the Internet. Another source of fragmentation is the growing level of geopolitical contention, particularly between Western regimes that favour the current open Internet and regimes of states pursuing a misguided vision of Internet sovereignty — erecting borders in cyberspace and asserting the government's right to impose significant constraints on the free flow of information on the Internet.[75]

These forms of fragmentation are costly for individual Internet users and for the global economy. Fragmentary legal systems requiring, as an example, local data storage threaten to expel financial services that cannot afford the costs. More generally, the restriction of the free flow of data tends to lead to significant reductions often over one percent, to a nation's GDP per capita with even larger reductions in investment exports and aggregate welfare.[76] At another level, state-imposed restrictions on content fragment the system and impinge upon the right of individuals to free expression.

The World Needs IPv6 to Meet the Demands of New Technologies and Emerging Markets

In the same way that streets use numbers to identify individual houses, the Internet uses unique virtual addresses to identify elements within its network. IP addresses are at the heart of how the Internet works, because routers use them to transmit information to its destination. The historic pool of 4.3 billion IPv4 addresses is exhausted — there are no more unallocated numbers. There are resource constraints in parts of the world without large reserves of IPv4 addresses.[77] Workarounds are creating complexity and security vulnerabilities. A new version of the protocol (IPv6) creates an enormously large reserve of available IP addresses (340 undecillion). While the standard has long been completed, it has not been extensively deployed, in part because it is not backward compatible with IPv4. Therefore, operators are forced to use workarounds to accommodate both IPv4 and IPv6. Particularly in the context of the IoT, the

Recommendation

The deployment of IPv6 by network operators is critical to the growth of the Internet. Governments and the private sector can play a leadership role in the wider implementation and adoption of IPv6 by promoting awareness and incentive programs in collaboration with the technical community. Governments should use their position as large ICT customers — for instance, by using their procurement policies to specify a requirement for IPv6 compliant products, software and network services. New applications, services and networks deployed by public agencies should be IPv6 compliant by default. ISPs and other network operators should continue to deploy IPv6 networks both for their customers and for upgrading their own infrastructure and services to be fully compliant. The Internet technical community offers best practices and guidelines accessible to network operators.

digital economy will greatly benefit from an effective transition to IPv6, due to the large number of objects that will become directly connected. Part of the collective action problem is that smaller players in the industry have limited economic incentive to upgrade their networks because they have a sufficient pool of IPv4 addresses for short-term growth. A sometimes neglected issue in Internet governance is the need to use practical policy and technical levers to ensure that the actual network can adapt to accommodate its explosive growth in both users and applications.

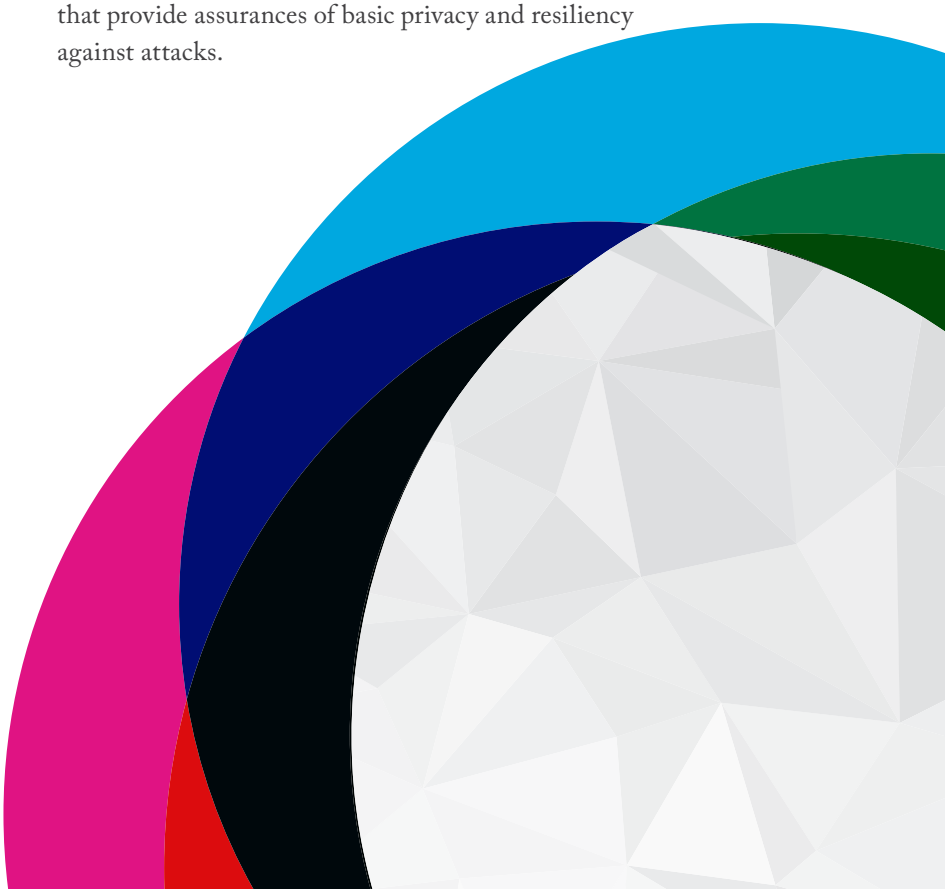
There Is a Critical Need to Retrofit Security Features into the Internet, New Technology and Applications

Before the globalization and commercialization of the Internet, security was not as critical a design consideration as it has since become in the era of the global digital economy. Even in the contemporary context, quickly deployed Internet applications often do not adequately address security requirements. This is the case, for example, in the realm of the IoT, where the imperative to ship early can outweigh extensive stress testing.

Some of the core infrastructural systems underlying the Internet require additional security retrofitting. The DNS, which associates numerical IP addresses with written names that humans can more easily understand, is an example. The original design of the DNS did not incorporate security features. Because of the significant role the DNS has come to play in keeping the Internet operational, it has been a frequent target for those seeking to disrupt Internet infrastructure. As in any piece of software code, many vulnerabilities can be exploited in the DNS.[78] One threat pattern involves malicious eavesdropping on DNS queries that resolve website names into IP addresses, and then falsifying the query response to redirect the web request to a counterfeit site that can then be used for identity theft, censorship or other malicious activity.

A new set of technical standards known as DNSSEC was designed to prevent these types of attacks by offering a method for cryptographically authenticating that DNS queries are returning the virtual location of the site a user intends to reach, rather than returning a false number that redirects the user to a counterfeit site. DNSSEC does not make the queries private, but rather addresses the problem of authentication, certifying that information returned originates from the legitimate site requested. Unfortunately, DNSSEC is not yet globally adopted and there is a need for simplification of tools and reduction of technical and other barriers to adoption.

As the IoT continues to expand into personal spaces from medical devices to homes and becomes increasingly embedded in every aspect of industrial and commercial environments, security will become more critical than ever. It is vitally important to not repeat the mistakes of the past. Considering the potential consequences of security incidents in the IoT, a higher level of security and privacy should be embedded by design. Trust in the Internet as a communication system, but also as an infrastructure that supports services that are essential to the functioning of the economy and society, requires security approaches that provide assurances of basic privacy and resiliency against attacks.



Recommendation

In the context of the IoT, avoiding the mistakes of the past requires a proactive approach to digital security risk management, rather than simply retrofitting patches after widespread implementation has taken place. As the expected global deployment of the initial IoT infrastructure is likely to be complete by early next decade, the urgency of the security task is pressing. Manufacturers involved in the value chain of IoT products should take responsibility for pursuing security in the design process. When bugs are found they must be held accountable for timely and effective patching when dealing with security vulnerabilities. Public policy has yet to catch up to these challenges and the security of embedded devices used in IoT products should urgently become part of national digital security policy frameworks.

Recommendation

DNSSEC offers significant improvements to the current security of the DNS. Even though DNSSEC is currently being deployed, it is not happening quickly enough. Accelerating its adoption should be considered a high priority by DNS and network operators. It is essential that the Internet technical community's ongoing promotion efforts continue to support operators with the deployment of DNSSEC through the promotion of capacity-building programs, best practices and guidelines.

Recommendation

All stakeholders should be informed by ISOC's Collaborative Security framework, which promotes five key principles: fostering confidence and protecting opportunities; collective responsibility; preserving fundamental properties and values; evolutionary steps based on the expertise of a broad set of stakeholders; and voluntary bottom-up self-organization.[79]

Recommendation

All stakeholders also should commit to a principled approach to their engagement in developing policies governing the Internet. The Commission supports the OECD's Principles for Internet Policy Making,[80] as well as the 2015 recommendations on Digital Security Risk Management for Economic and Social Prosperity.

OECD INTERNET POLICY MAKING PRINCIPLES

1. Promote and protect the global free flow of information
2. Promote the open, distributed and interconnected nature of the Internet
3. Promote investment and competition in high-speed networks and services
4. Promote and enable the cross-border delivery of services
5. Encourage multi-stakeholder cooperation in policy development processes
6. Foster voluntarily developed codes of conduct
7. Develop capacities to bring publicly available, reliable data into the policy making process
8. Ensure transparency, fair process and accountability
9. Strengthen consistency and effectiveness in privacy protection at a global level
10. Maximize individual empowerment
11. Promote creativity and innovation
12. Limit Internet intermediary liability
13. Encourage cooperation to promote Internet security
14. Give appropriate priority to enforcement efforts

Source: www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf.

OECD DIGITAL SECURITY RISK MANAGEMENT

General Principles

1. Awareness, skills and empowerment: All stakeholders should understand digital security risk and how to manage it.
2. Responsibility: All stakeholders should take responsibility for the management of digital security risk.
3. Human rights and fundamental values: All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.
4. Cooperation: All stakeholders should cooperate, including across borders.

Operational Principles

5. Risk assessment and treatment cycle: Leaders and decision makers should ensure that digital security risk is treated on the basis of continuous risk assessment.
6. Security measures: Leaders and decision makers should ensure that security measures are appropriate to and commensurate with the risk.
7. Innovation: Leaders and decision makers should ensure that innovation is considered.
8. Preparedness and continuity: Leaders and decision makers should ensure that a preparedness and continuity plan is adopted.

Source: www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/OECD_digital-security-risk-management_0.pdf.

Recommendation

When a security or design flaw is discovered in technical protocols, there should be rapid response procedures within a standards institution to quickly and effectively address the vulnerability. When a design flaw is discovered in applications in the IoT or other commercial software, industry should have similar rapid response procedures.

Government Policies That Tamper with Infrastructure Can Have Negative Externalities

Another trend that is producing destabilizing effects on Internet infrastructure stability is the movement by several world governments toward passing laws and imposing policies that mandate modification of the Internet's infrastructural configuration, not for efficiency or technical redundancy, but to achieve other objectives. In many cases, the objectives are well meaning, such as the protection of citizens' personal information. In other cases, the objectives of these modifications include censorship and indiscriminate surveillance.

One example of how governments can attempt to impose infrastructure modifications to achieve their goals can be loosely described as "data location" or "data localization laws." In the past few years, several countries have established data localization policies that impose restrictions on how corporations store, process and transmit customer data across borders. These laws apply to large Internet intermediaries, such as search engines, and also companies across industry sectors, such as multinational financial services companies whose services and customers are located

around the world. James M. Kaplan and Kayvaun Rowshankish in GCIG Paper No. 14 describe the types of restrictions arising in this new regulatory context and also warn about the potential negative effects on the ability of transnational corporations to efficiently and securely conduct routine business transactions.[81] Some of these effects include: the requirement for increased organizational complexity to manage these requirements; lower efficiency; a company reduction in global footprint, which can in turn affect emerging markets; and constraints on technical architecture strategy.

Requiring data localization can contribute to achieving national or regional public interest objectives, but can also constrain the infrastructure decisions necessary for market-efficient and technologically sound business approaches. For example, there are obvious public interest rationales to prohibit the storage of sensitive government data on servers located in other countries. But for more general communications, efficient and valuable flows of data can be undermined by politically driven localization constraints. Greater respect for the privacy of foreign citizens' data would weaken incentives for such data localization approaches and international cooperation on this issue would be valuable. One example of this is the 2016 move by the United States and Europe to negotiate new Privacy Shield principles to replace the now defunct Safe Harbour Framework. Moves such as this could help to protect user data that flows between countries and diminish the incentive to implement data localization legislation.

Open Standards and Interoperability Should Be Preserved as Drivers of Innovation and Security

Increasingly, actors in the marketplace are promoting proprietary approaches, ranging from the use of Application Program Interfaces rather than open standards to the private sector zero-rating services that only provide access to selected services (walled gardens) rather than the Internet as a whole. In the former case, some standard-setting processes may be seen as too slow by companies that are eager to launch products. There is a recognition that Internet standard-setting processes need to be shortened to meet the demands of fast-paced markets. Collaborative processes are critical for democratic legitimacy but, pragmatically, collaborative processes cannot be endless. Market forces are fast while standardization processes can be slow. This context can have effects on Internet security and stability because fast-paced markets in which security and privacy are afterthoughts can create inherent vulnerabilities.

A standards consideration related to security is that protocol security has historically been advanced, in part, by transparency. A specification that is open to inspection and developed and implemented by multiple interests is more likely to have its security vulnerabilities discovered and mitigated. Movements to proprietary approaches forestall this collaborative security norm.

Recommendation

Policy makers also need to acknowledge the technological and economic complexities around data location decisions and aim to avoid requirements that would undermine the technical interoperability, openness and distributed design of the Internet.

Recommendation

It is imperative that all stakeholders recognize that parts of the Internet are, in effect, a shared global resource, and thus should not be subject to interferences that could harm the infrastructure of the Internet.

Distributed Governance Can Preserve Open and Stable Internet Infrastructure

As previously noted, policy makers have a responsibility to promote Internet infrastructure stability, but they are only one set of actors involved in coordinating Internet infrastructure. Internet infrastructure is an ecosystem of technologies, systems, institutions and actors. The governance of this infrastructure is — and should be — distributed, and employ "more collaborative, global and decentralized models of decision making," as Stefaan G. Verhulst et al. argue in GCIG Paper No. 5. Characteristics of this model would include:

- enhanced coordination and cooperation across institutions and actors;
- increased interoperability in terms of identifying and describing issues and approaches for resolution throughout the ecosystem;
- open information sharing and evidence-based decision making; and
- expertise- or issue-based organization to allow for both localization and scale in problem solving.[82]

In this context, it is not necessary for all actors to simultaneously oversee or participate in every aspect of Internet infrastructure governance. Rather, responsibilities are both distributed and collaborative. Opportunities for enhancing the stability and openness of Internet infrastructure include improving inclusion and human capacity building in the institutions that administer technologies such as numbering systems, interconnection points and standards setting. It also involves capacity building in the administration of the underlying technologies undertaken by these institutions and by private companies. For example, IXPs are basic building blocks necessary to accelerate Internet access, improve the efficiency of traffic exchange, reduce costs and increase the stability and reliability of the Internet at the local, regional and global level. Due to global routing economics, low demand for digital services and other non-economic reasons, some regions do not yet have enough IXPs, and this gap limits the opportunity of developing a digital economy.

Another essential element lies in the existence and stability of the organizations responsible for development of open standards and protocols for the Internet. Key technical institutions, such as the IETF and W3C, depend almost entirely for support on voluntary contributions of knowledge and resources provided by corporations and individuals committed to their work. This may not always be sustainable, particularly as the pioneers who established and remain key supporters of these bodies disappear from the scene.

Recommendation

Open standards that are transparent and allow multiple interests to participate on a voluntary basis should be the norm rather than the exception to help reduce design flaws and to promote innovation.

Recommendation

Governments should provide incentives for the implementation of open standards and for services that do not impose artificial walls around the information citizens can choose to access. Because governments are such large purchasers of information and communication technologies, procurement policies are an effective method for creating incentives.

Recommendation

Governments and the private sector need to develop creative mechanisms to provide sustainable funding for the Internet's key standard-setting organizations.

Encouraging Leadership from the Technical Multi-stakeholder Community

Internet infrastructure, while considered a shared public resource, is largely privately owned and technologically complex. Nonetheless, as this report suggests, it embodies design and coordination decisions with significant public interest implications ranging from privacy to security and, ultimately, the continued viability of the Internet itself. IANA functions, such as the coordination of technical IP parameters, certain responsibilities associated with the DNS root zone management and the allocation of Internet numbering resources, are certainly part of the shared global public good of Internet infrastructure. Routing infrastructures, IXPs, electromagnetic spectrum and the protocols that enhance security and privacy are also part of the public good.

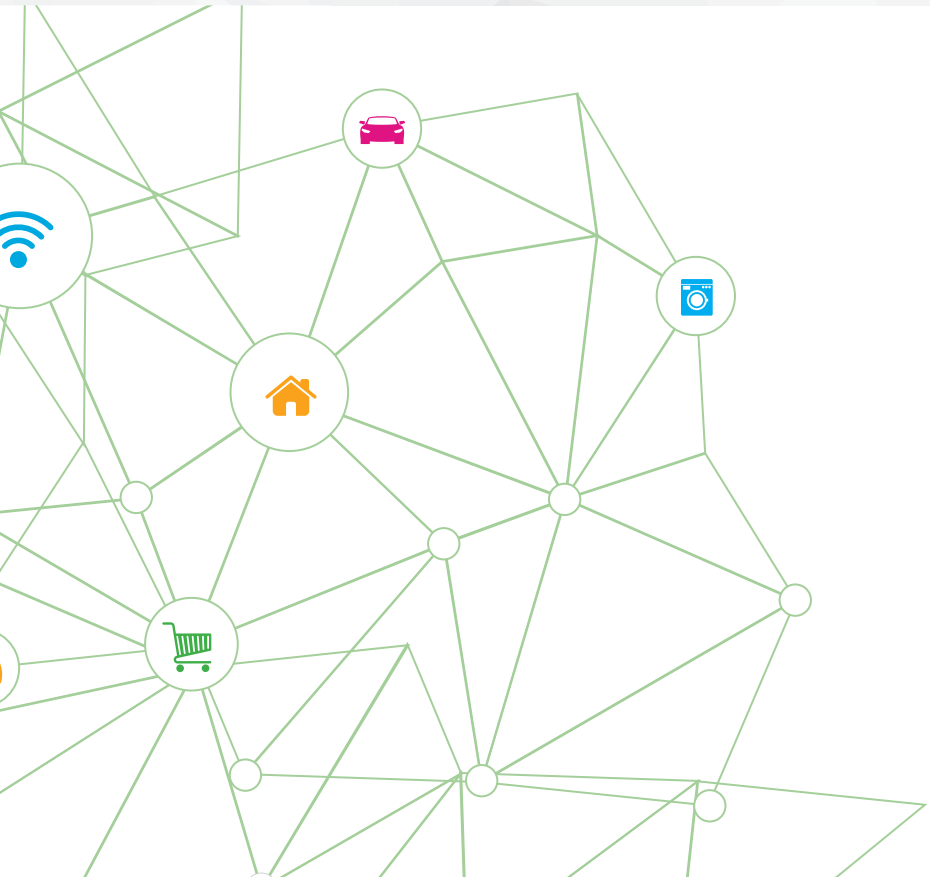
The responsibility for these core infrastructure technologies resides in the technical multi-stakeholder community, which assumes the responsibility for promoting approaches to coordination and design that embody principles of openness, security and innovation.

Recommendation

All stakeholders should work to keep the IANA functions, such as the coordination of technical Internet protocol parameters, certain responsibilities associated with the DNS root zone management and the allocation of Internet numbering resources, in the technically focused multi-stakeholder community and adopt a model in which no single interest can capture control.

Recommendation

Network operators should fulfill their responsibility to Internet users by putting in place current clear security protocols for routing resiliency.



Reducing Crime in Cyberspace

In recent years, activity on the Internet has exploded as its commercial and social advantages have been recognized. Now, the Internet is viewed as the "infrastructure of infrastructures." Increasingly, global trade and economic development, innovation, public administration and the free expression of individuals all depend upon the functioning of the network. By any measure, the Internet is an incredibly useful tool. Unfortunately, as the Internet has grown in its power and reach, other more nefarious actors have recognized the utility of this tool and now use it to prey upon people around the world. As in the off-line world, crime is a global problem in cyberspace.

Efforts to combat cybercrime are often hampered by political and technological problems. Cybercrime transcends borders with unparalleled freedom. Policing across borders is far more challenging than attempting to combat crime within a single state's borders because it requires international cooperation. The architecture of the Internet also hampers cybercrime investigations, since it can be quite difficult to pinpoint the location and identity of the perpetrators of cybercrime.

Some research even suggests that the annual costs of global cybercrime could surpass the annual benefits of the Internet by 2030.[83] This future is not guaranteed, but should it come to pass, it is possible to imagine that people could stop using the network for commercial transactions or personal communications. Law enforcement, governments and other stakeholders — including ordinary individuals — need to work together if this drastic outcome is to be avoided. A starting point is the broad-based improvement of everyone's digital hygiene, such as downloading software patches, changing passwords and not clicking suspicious links. By some estimates, such simple steps to improve our digital hygiene could address between 80 and 99.9 percent of all cyber attacks.[84]

Types of Crime

Crime and criminal acts increasingly occur online. As a network that covers the world, the Internet has created a window where online criminal behaviour has flourished. The interconnected nature of the Internet has allowed criminals of all stripes to launch a wide range of criminal activities, such as fraud or identity theft, on ever greater scales.

Criminals are growing very adept at gaining access to devices and using that access for their own ends. Sometimes they steal information, such as credit card details, passwords and private photos. At other times, that access is used to commandeer a person's system so the device's processing power can be harnessed to launch distributed denial of service (DDoS) attacks against banks, government websites and other critical infrastructure. At the extreme, DDoS attacks might cost as much as $920 million globally per day.[85] Increasingly, criminals have also started to use ransomware attacks, using encryption to lock a person's device and then demanding payment of a small ransom in exchange for the keys to unlock the system.

Criminals also take advantage of industries' ubiquitous use of the Internet to steal corporate secrets and intellectual property. Companies have routinely failed to protect their systems against data breaches both at the level of corporate policy and through sloppy digital hygiene on the part of their employees. In many instances, the problem is exacerbated by the close links between malicious hackers and state governments. State-sponsored hackers are particularly effective at pilfering secrets as they go about their economic espionage.

Online crime can also be surprisingly personal, with online bullies aiming to wreck people's lives, often by "doxing", "trolling" or distributing personal information about a person. While anyone can be bullied online, the problem is particularly acute for women and girls. Women are already more likely to be sexually assaulted or stalked than men are. Both the anonymity of online interactions and the disinhibition that comes with sitting behind a computer screen can further exacerbate this social problem. Women and girls are subject to various forms of online criminal behaviour, ranging from stalking to being the victim of so-called revenge pornography.

An increasingly large amount of online crime and criminal behaviour is facilitated by the Dark Web, which is really the shadowy underbelly of the Internet.[86] Anonymity is the defining feature of the Dark Web. Criminals use the anonymity of the Dark Web to organize conspiracies, launder money and contract illegal services, such as assassination for hire or the use of botnets to launch DDoS attacks. Illegal marketplaces such as Silk Road exist on the Dark Web, connecting sellers of drugs and guns with consumers. The websites on the Dark Web are mostly not indexed, and cannot be accessed by commonly used web browsers such as Google Chrome or Safari. Instead, people wishing to access or host websites on the Dark Web need to use specially configured systems. The most commonly used system to both connect to and host content on the Dark Web is called The Onion Router — or Tor for short. Tor encrypts and then breaks up a person's Internet connection, providing the closest possible thing to online anonymity, affording cover for what they do there. The cover of online anonymity can cut both ways. While Tor can be used by individuals in repressive regimes to circumvent censorship and avoid surveillance, it is also used by criminals taking advantage of the Dark Web that it helps to create.[87]

Many people use Tor as a web browser for everyday content to ensure anonymity. However, some users also host websites on Tor known as "hidden services." A large amount of Dark Web activity is dedicated to these hidden services, which include websites that allow for the distribution of child pornography, including child abuse imagery. As Gareth Owen and Nick Savage reveal in GCIG Paper No. 20, while only around two percent of all Tor Hidden Services websites host child abuse imagery, 83 percent of the actual site visits go to this small fraction of websites.[88]

As with conventional criminals, terror groups are also turning to online platforms to organize their attacks with increasing frequency.[89] Terror groups also use content-hosting platforms such as Twitter and YouTube as dissemination tools for their propaganda. This illicit use of common online services has put companies and governments at odds, often with companies playing the

champion of an individual's rights to free expression and online anonymity, while some governments call for "backdoors" in hardware and software, and even an end to online anonymity

This issue has been a major concern recently with the skillful use of the Internet by Daesh/ISIS to spread their propaganda, recruit "jihadists," and attract and radicalize individuals from around the world to join their groups.

Similarly, several recent cases have highlighted the tension between governments and companies over access to encrypted equipment and data in cases of known terrorist activities. These examples of competing legitimate interests once again raise the question of how to balance the needs of law enforcement and security agencies against the need to ensure the integrity of encryption for commerce and the protection of individuals' privacy.

Overall, the Internet has greatly improved many people's lives. It has generated wealth, improved the efficiency with which services can be rendered, and improved access to information and social activities. But it has a clear downside in online crime. The forms of online crime are numerous, varied and damaging to the trust and confidence that people must have to be comfortable and safe using the Internet.

Trends in Crime

By virtually every measure, the absolute amount of criminal activity that has been occurring online is increasing year over year. The volume of online attacks, the number of ways an interconnected device can be attacked and the costs of those attacks are evidence of this trend. For example, the IT security firm Kaspersky Labs has collected data on the number of web-based cyber attacks from 2008 to 2014 and found a nearly consistent year-over-year increase in the total number of attacks, reaching as high as 1.7 billion attacks in 2013.[90] Other IT security companies such as Norton Symantec collect data on the generally growing number of vulnerabilities in computer software and firmware. For example, according to Symantec's annual "Internet Security Threat Report," the number of new vulnerabilities identified each year has grown from 5,562 in 2008 to 6,549 in 2014. Among a number of other speculative predictions of the costs of cybercrime, the IT security firm McAfee (a division of Intel), in collaboration with Center for Strategic and International Studies, contends that cybercrime costs the global economy somewhere between $375 and 575 billion per year.

Even taking into account the difficulty of estimating the frequency and cost of cybercrime in the absence of robust internationally comparable indicators, the general trend indicated by these estimates points toward a worsening situation in cyberspace. However, absolute numbers do not tell the entire truth, so one should temper the alarm such estimates might engender. Estimates of cybercrime are usually expressed either as a count (1,000 crimes last year and 1,500 this year) or as a year-over-year percentage change based upon these figure (50 percent more attacks this year than last year).** This measurement by simple counting contrasts with how we measure crime in the off-line world. Off-line criminal activity is always expressed as a rate of crime (the number of crimes divided by the population that can be affected).

Recommendation

Governments should initiate efforts to develop international consensus on norms about how to deal with cases where the goal of protecting data comes into conflict with the requirements of law enforcement or security agencies to investigate terrorist activity or attacks in an emergency situation. At a minimum, any solutions should be derived through a multi-stakeholder process, broadly agreed, and must be subject to legal oversight, governed by principles of necessity, proportionality and avoidance of unintended consequences.

** A notable exception is the UK Office for National Statistics, which expresses cybercrime numbers as a proportion of the domestic population.

To better capture trends in cybercrime, the same measurement system should be used in cyberspace.[91]

If cybercrime is measured as a proportion of the number of Internet users, the situation looks less alarming. As we know, Internet use is growing rapidly year-over-year. As we would expect with a growing population of a physical city, the total number of crimes online should go up as the population of cyberspace grows and as users become more active, even if the rate of crime remains constant or even falls. Empirical research shows that this indeed is what is happening. For example, while the absolute number of web-based attacks recorded by Kaspersky Labs declined by 15.77 percent from 2013 to 2014, the number of attacks normalized around web traffic started declining one year earlier — in 2012 — and declined by 40.55 percent from 2012 to 2014. This is not to say that the situation is improving or even acceptable, only that a fixation with the raw number of attacks presents a distorted view of the reality of the situation.

Better measurement based on more robust indicators will provide a firmer foundation for legal frameworks and policies designed to counter cybercrime. It will also allow for a better after-the-fact evaluation of whether a particular policy innovation is having a desirable effect. One thing is certain: no matter how it is measured, crime remains a problem. States, private companies and ordinary Internet users all recognize the growing problem of cybercrime and that they need to work collaboratively to counter online criminals.

To collect accurate statistics, a mandatory requirement for notification of data breaches is a key element. Companies are often hesitant to reveal that they have been hacked, as they are concerned about how consumers might respond to news of these intrusions. However, mandatory notification has three positive benefits: it pressures boards and senior management to manage for cyber-security risk; it provides risk-related data that industry can use to conduct risk analysis for new cyber-risk products, including insurance; and it improves consumer trust by making risk-related data and analysis transparent. As with health problems, public reaction is likely to be most severe when there are only a few isolated cases. Once the public comes to understand that every company can be breached, the public backlash will be moderated and attention will shift to how the company manages the aftermath of the breach.

Recommendation

Governments should draft legislation that requires the mandatory public reporting of high-threshold data breach details.

Responses to Crime

Governments, private companies and individuals can all take reactive actions to counter crime in cyberspace, but there is a broad-based need to improve the general state of digital hygiene around the world in order to combat crime through prevention. In 2009, a US Senate hearing revealed evidence that upwards of 80 percent of cyber attacks could be prevented by proper system configuration and network monitoring.[92] Even something as simple as downloading and installing patches for commonly used software such as Microsoft Word or Adobe Flash can have a drastic effect on the ease with which criminals can exploit the technology for malicious purposes. According to Verizon's "2015 Data Breach Investigations Report," for example, upwards of 99.9 percent of vulnerabilities were exploited one year after the vulnerability had been exposed and recorded in the Common Vulnerabilities and Exposures database, and thus occurred one year after patches were available for the exploit.[93] Simple improvement in digital hygiene can prevent a lot of criminal behaviour in cyberspace, thereby freeing up governmental and private resources that could be used to contend with more sophisticated threats.

Proper digital hygiene hinges upon the widespread availability of the information needed to keep people safe. There are several welcome efforts already at work to try to collect and coordinate the sharing of information and best practices across borders, such as initiatives such the Global Cybersecurity Index,[94] the Cyber Readiness Index[95] and CyberGreen.[96] Efforts of this sort need to be broadened and deepened as

much as possible if cyber hygiene is to prove to be a truly effective preventive tool against cybercrime.

Being realistic, it has to be said that currently and in the short-to-medium term, efforts at improving digital hygiene alone will likely not be sufficient to make cyberspace safer. As a result, governments, private companies and individuals sometimes need to undertake steps to combat crime in a more reactive fashion. While the need for these efforts can be greatly reduced by better digital hygiene, the reactive measures themselves are proving to be only marginally effective in most cases.

In a world of sovereign states, governments have traditionally had the practical responsibility for policing society. Increasingly, as online crime has become a more endemic problem, governments have generally increased the resources and effort devoted to policing cyberspace. Some early successes include instances of successfully apprehending online child predators and the arrest of those involved in illegal marketplaces, such as the high-profile Silk Road, and the takedown of botnet computer networks used to attack critical infrastructure. Both old-fashioned police work and the innovative use of new technologies are needed to police the Internet in the digital age.

Effective policing in other areas is far less effective. State efforts to police cyberspace are usually limited by problems resulting from the fact that cybercrimes often span geographical jurisdictions, thus requiring international coordination, and demanding more resources. Another limitation involves the often significant lag between the development or reform of laws that govern what is legal or illegal online, and the pace with which the technology changes and shifts in people's use of the system.

The law reform process has not sped up sufficiently, but recent moves have been made to update laws so that they protect people from online abuses, such as banning so-called revenge pornography in many US states. These are all positive steps, but they have not proceeded far enough or quickly enough. It is likely that, at least for the foreseeable future, law will always lag technology, but this does not mean governments should just accept this as unavoidable. Instead, they should make greater effort to ensure that laws react in a timely manner to challenges emerging in the digital ecosystem.

Cybercrime and cybercriminals traverse space with unparalleled speed. Cybercrime has localized victims, while the perpetrators very often reside in very different jurisdictions around the world. Finding the perpetrator of a cybercrime and getting a conviction almost always requires that various law enforcement bodies carefully coordinate their efforts. At best, this coordination will be within a single country, with local law enforcement coordinating with subnational and national police services. Often, however, the coordination will have to be across national borders. Law enforcement agencies need to better recognize that cybercrime very often cannot be dealt with locally and will cross into different organizations or countries' jurisdictions. Formal procedures for facilitating coordination, such as deciding on a basic rule regarding the organizational lead in an investigation, are essential. Getting broader participation in these positive efforts started at Interpol's i-24/7 data exchange initiative would go a long way toward improving the ability of law enforcement to apprehend cybercriminals across borders.

In response to these challenges, governments have been increasing both national and international

If cybercrime is measured as a proportion of the number of Internet users, the situation looks less alarming.

coordination, devoting more resources to combatting cybercrime — often establishing dedicated units to do so — and seeking reform of the mutual legal assistance treaty (MLAT) process.

Overwhelmingly, cybercrime will span borders. MLATs are meant to assist nations that need to pursue a criminal across national boundaries. In today's world, MLATs are cumbersome, and can take up to a year to complete, even if one excludes the number of applications rejected because of process issues. The requests for assistance are often thwarted by a lack of compatible legal requirements in the correspondent countries. To take one example, unless required to do otherwise, most ISPs only retain data for between six months and one year, which means that the data that a government is looking for might be deleted even before the MLAT process is completed. The inefficiency of MLATs is a serious impediment to law enforcement's efforts to combat cybercrime. Governments need to work to reform the process so that seeking legal assistance from other states is easier, more transparent and faster.

Law enforcement is at the front line in combatting cybercriminals, but law enforcement agencies remain woefully under-resourced and often lack the skills and training needed to effectively contend with sophisticated online criminals. Without additional resources, law enforcement agencies will find it difficult to bring the necessary capacity to bear upon the problem at hand.

Combatting cybercrime would be far simpler if all nations agree upon some basic definitions of online criminal behaviour and harmonized their national laws to ensure that as many jurisdictions as possible had comparable laws. One early effort in this regard was the Budapest Convention on Cybercrime. Now in force in 48 countries stretching from Europe to the Americas, Africa and the Caucasus, and the Pacific the convention goes a fair way toward making cybercrime illegal in all jurisdictions. However, several states that have an active cybercrime element are not parties to the treaty. Current signatories should expand their efforts to make the Budapest Convention more inclusive, to improve government cooperation on combatting the scourge of cybercrime.

While states have been the main law enforcement body in our current Westphalian era, there is an increasing trend toward policing being undertaken by states in close collaboration with private companies. For example, "Operation Tovar," which took down the expansive ZeuS botnet, was achieved by a combination of the FBI, Europol and the UK National Crime Agency working in concert with a host of private companies, including Crowdstrike, Dell SecureWorks, Symantec, Trend Micro and McAfee. This takedown is but one example of the close, and often highly effective, collaboration of governments and private companies in the policing of cyberspace. Computer Security Incident Response Teams are also an invaluable bulwark in the collective fight against cybercrime.[97]

Recommendation

Apprehending criminals across national borders remains a difficult challenge. Governments should never purposefully shelter those that have been linked to the commission of cybercrimes.

Recommendation

The transborder nature of many significant forms of cyber intrusion curtails the ability of the target state to indict, investigate and prosecute the individuals or organizations responsible for that intrusion. States should coordinate responses and provide mutual assistance in order to curtail threats, to limit damage and to deter future attacks.

Recommendation

States should not rely upon the weaker data collection rules that govern private companies to get access to information that they could not obtain themselves through legal channels.

THE DIGINOTAR SCANDAL

The Diginotar scandal illustrates why the two-fold dependency on private companies leads to serious concerns. The Dutch government relied on Diginotar to provide security certificates for most of the electronic services it provided, including sites that had been used for all online tax returns filed in the Netherlands. After the company's infrastructure had been breached, fake certificates were issued for hundreds of popular websites, which could be used to launch man-in-the-middle attacks. An investigation by another private company provided evidence that the false certificates were used to monitor the communications of approximately 300,000 Internet users in Iran. After the attack, the company did not report the incident immediately, thereby jeopardizing the security and privacy of not only Dutch Internet users, but millions of other Internet users across the globe. How healthy is a situation in which the security of our communications online depends on a cyber-security company whose most critical servers contained malicious software that can normally be detected by anti-virus software?

Such collaboration can be useful for two reasons. First, private companies such as ISPs and content platforms own and operate a lot of the physical infrastructure of the Internet. Second, private companies are often best positioned in terms of technical skills and resources to identify criminals and to track and destroy (or at least contain) malicious code. These realities entail an expanded role for private companies in the policing of the network, often in collaboration with governments.

Increasingly, law enforcement in cyberspace is not the sole purview of governments. Governments often work in close collaboration with technology companies to bring down botnets and otherwise police cyberspace. In principle, both governments and technology companies should be receptive to these public-private partnerships. In practice, these coordinated efforts should not be used by either side to circumvent any legal restrictions that might be in place.

Private companies that are not directly involved in the IT space are also often thrust onto the front line of defence against cybercrime. Companies ranging from Home Depot to Target to eBay have had their systems breached and customer data stolen. These data breaches, and all the unreported attempted breaches, against companies are growing frighteningly common. Sometimes these breaches are tied to state-sponsored hackers in foreign countries, as in the case of the attack against Sony Pictures Entertainment in 2014 by "The Guardians of Peace." Sometimes these attacks come from private sector actors, such as the hack of the online adultery site Ashley Madison, by the group or individual going by the name of "The Impact Team."

Many private companies have responded to their real and perceived vulnerability by establishing a chief information officer position, with the responsibility to coordinate cyber defence. According to a recent C-Suite Survey of executives, over 60 percent of businesses have also increased their IT security budgets due to the perception of a worsening security environment.[98] These efforts are a set of good first steps, but most companies have relatively immature processes for making and implementing decisions about how to protect themselves from cyber attacks.

The knowledge about operating and securing data systems, software and networks is overwhelmingly in the hands of private cyber security companies, which are used by governments to protect themselves against cyber attacks, and their inhabitants against various forms of cybercrime. Outsourcing online security to private actors without clear oversight and control regimes amounts to negligence.[99]

Businesses are the cornerstone of national economies. More and more, states and companies are relying upon efficiency-enhancing digital technologies that are vulnerable to cyber attacks. Businesses have to

take seriously their responsibility, to their owners and employees, to secure the future of the business from cyber attacks, including information theft and data corruption. They must also be vigilant in discharging their responsibility to their customers for safeguarding their information so that private and secure services can be provided. Businesses must invest not only in enhancing their cyber defences, but also in building security into their underlying business processes and technology architectures.

Unfortunately, SMEs which form the backbone of the global economy may not be financially capable of shouldering the burden of extensive IT security, or may not see it as a priority use of limited resources. However, even small companies can be a threat vector for their customers or their commercial partners. Systems breaches of larger companies can come from anywhere in their supply chain, as evidenced by the breach at Target via an HVAC vendor.

Governments have a responsibility to reach out to their SMEs, including working with the cyber-security industry and the insurance sector, to explore funding routes and capacity-building efforts that can assist smaller companies in managing digital security risk in an effective manner for the benefit of all.

The responsibility of a business does not stop at simply trying to prevent a cyber breach of their systems. Companies also need to be prepared to deal with the consequences of a successfully executed cyber attack, and should find ways to share what they learn in the process without compromising their competitive positions.

Cyber liability insurance vendors can also be persuasive in promoting best practices in the corporate sector. Cyber premiums can be expected to be higher if best practices are not followed, just as health premiums or vehicle insurance premiums are affected by what the policyholder does or does not do. The market for cyber insurance is immature in comparison to the seriousness of the threats, and the capital available to the industry is currently inadequate to underwrite the full risk. Pricing the risk is difficult in the absence of reliable time series data, making it difficult for insurers to put a reliable figure on the likely losses from breaches.

Despite its current limitations, risk markets (including bond markets) can play a major role in building resilience among individual and business users. Public reporting of cyber attacks and their impacts (even if the report is anonymized) will enable the risk markets to develop fact bases on which to price cyber risk products. In other areas of insurance, the reliance on third-party evaluators of ICT products helps to reduce systemic risk. Third-party evaluation processes are needed in ICT supply chains, although corporate compliance with such evaluation standards will not be sufficient for enterprise security.

Recommendation

Businesses should purchase cyber insurance to cover the liability costs of successful breaches of their systems.

Recommendation

More research is urgently needed to support greater accuracy when pricing risk. This is an area where the OECD could make a significant contribution.

Recommendation

To assist the public to understand and practise the essentials of cyber hygiene, governments should undertake significant campaigns to raise awareness and develop the needed skills. Cyber-security awareness programs should start early, for example, by incorporating cyber hygiene into primary and secondary education curriculums.

In the end, ordinary individuals are both the most common target of cybercrime and in the best position to defend themselves, whether in their homes or in their professional lives. Certainly, some people have responded to the real and perceived dangers of cyberspace by being more cautious about what they do online, thereby protecting themselves (and others) from cybercrime. Yet, many individuals do not follow even the bare minimum standards of digital hygiene, such as changing passwords regularly, not clicking unknown links or using antivirus software, thus endangering themselves and others.

A large majority of data breaches are the result of human error. People are the weak link in most IT security systems. Law enforcement and private companies need to do their best to protect users, who are generally less knowledgeable about how cybercrime unfolds. Capacity-building efforts to develop cyber-security skills are crucial for preventing crime online, but they are often adversely affected by cumbersome political institutions and cultural issues.[100] Everyone needs to recognize that sometimes they are themselves the last and best line of defence against cybercriminals.

The reality is that the Internet ecosystem is populated by calculating and reactive actors. Criminal elements adapted to the growth of the Internet by increasing their online presence and expertise, often capitalizing upon the weaknesses of others. Governments, private companies and individuals have had uneven responses to cybercrime. The responses that have been undertaken have been patchy and very shallow in some areas. Crime has always been an endemic social problem and the core lessons of the off-line world apply online: crime in cyberspace can be made less pronounced than it is today through the exercise of common sense, by undertaking tried and tested precautionary measures, and by judicious policing.

Developing New Norms for Geopolitical Relations

States around the world are shifting more of their essential services and government functions online, including the crucial components of their national defence. Modern militaries are increasingly reliant upon global communications platforms, including the Internet. Finance and commerce, the backbones of almost every economy, are increasingly based upon Internet-enabled infrastructure. Large portions of critical infrastructure, ranging from power grids to airports and pipelines to hospitals, are now linked to the Internet. As states shift more of their activity online, geopolitical contention has followed. While progress has been made and all is not lost, norms in cyberspace to restrain state actors' use of cyber weapons remain underdeveloped. The problem of large-scale interstate cyber conflict should not be overblown, but cyberspace is certainly increasingly being used for state-originated or -sponsored espionage, sabotage and other destructive purposes.

Governments and companies are also storing an ever-larger amount of valuable and sensitive information online, including citizens' personal data and intellectual property, in order to improve the efficiency with which services can be provided. In doing so, however, they potentially expose the data to hostile state attack. The aim of those attacks can be to steal information relating to national security, to disrupt services, to deny services or to corrupt data leading to a loss of confidence in the systems concerned. So-called "Trojan Horse" attacks can be planted within systems to lie dormant until called upon by their masters, such as in a crisis when armed conflict appears inevitable. What makes such attacks especially tempting is the prospect that they can be covered by plausible deniability due to the technical difficulty of attributing the attacks. Broadly speaking, cyber activity by governments and other malicious actors can be divided into two categories: computer

network exploitation (designed to view or steal information) and computer network attack (designed to disrupt or damage the operation of digital systems. So far, we have seen a lot of the former and only a little of the latter, but that could change.

Preventing such cyber attacks against a country's digital assets is difficult because there are many vectors by which a non-state or state-sponsored agent can gain access to a computer or network server in order to deliver a payload or malicious outcome. The first vector is along the network itself. Such attacks range across a broad spectrum from relatively unsophisticated DDoS attacks to highly sophisticated malware attacks that exploit or introduce flaws in the software and algorithms on which networks rely. The second vector of attack is via the supply chain. States and companies can implant malware or firmware during the production or installation of IT and communications systems that can then be exploited by governments or non-state actors. The third vector of attack is social. Human behaviour is usually the weakest link in any IT security system. Many successful attacks get into targeted systems thanks to their perpetrators' effective use of social engineering to trick individuals into accepting infected communications, rather than because of any inherent technical weakness in a target's IT infrastructure. The spread of cloud computing and of the IoT will increase the number and type of opportunities for penetration available to an attacker. The offence has the advantage over the defence today, and this asymmetry is likely to continue for the foreseeable future.

The heightened reliance upon Internet infrastructure as the means of transporting digitized information, and its vulnerability to multiple vectors for cyberattack, has led to a situation where governments and non-state actors increasingly turn to cyberspace to act out their geopolitical differences. If not properly checked by widely agreed norms of behaviour, serious consequences seem likely to result. One example of the type of damage that could be done if adequate norms are not developed and agreed upon now, is the January 2016 attack on Ukraine's power grid that left 80,000 people in western Ukraine without power. States around the world need to come together to ensure that our digital future is not fraught with perils and tribulations.

The Causes of the Growing Hostile Use of Cyberspace

The global militarization and other hostile uses of cyberspace is enabled by several factors, most notably the inherent technical insecurity of the Internet, the problems of attributing and tracking down the perpetrators' cyber attacks, the dominance of the offensive, and the decoupling of motive and ability. Each of these factors are described in more detail below.

Attribution Problems

One primary cause of the temptation to engage in aggressive interstate activity in cyberspace is the difficulty of pinning down, to a sufficient standard of proof, which state or group is behind a particular attack. This issue is commonly known as the attribution problem. There are many ways for malicious actors to mask their identities or to pose as someone else. Attacks can be relayed through a number of different computers all over the world before they actually try to breach a government's network, making it difficult to retrace steps and assign blame. Malware can be written to mimic the signatures that would be seen in attacks by other actors. A less technologically savvy attacker can simply use a computer in an Internet café or coffee shop with a public Wi-Fi connection to launch an attack, including from within the nation being attacked, obscuring the real origins of the attack and complicating any investigation. Some nations even outsource their attacks by essentially renting freelance hackers or encouraging cyber-criminal gangs to attack another nation's financial system. There are many ways of keeping the real source of the attack at arm's length from forensic discovery, providing plausible deniability to any assailants.

Technical attribution is difficult and, even when an investigation appears to point to a probable culprit, the possibility of deliberate deception has to be considered. This is increasingly the case as knowledge about cyber forensic techniques spreads. It may, nevertheless, be possible for intelligence analysts to provide an assessment of likely attribution based on

other evidence and on specific intelligence. A case in point was the attribution by the United States of the attacks on Sony Entertainment to North Korea, which combined multiple data sources, both technical and human, to construct a plausible case for attribution.

Once an intelligence agency believes it has identified a culprit, the government of the attacked state must consider whether action should be taken against the state or individuals believed responsible, and whether evidence is sufficiently strong to merit laying criminal charges (as the United States did with its indictment of five Chinese People's Liberation Army officers in 2014). The judgment of what action to take also has to consider the possible negative consequences of accusing another state openly, especially if such an accusation would put sensitive intelligence sources at risk. Despite its technical elements, the admission of having suffered a cyber attack and accusing a suspect become a problem that is primarily political in nature. The burden of proof varies depending upon how a government wants to respond. Generally, attempting to lay criminal charges against cyber attackers requires a higher burden of proof than rhetorically attributing an attack to a particular actor (as in the case of the United States with North Korea following the Sony Entertainment attack).

States retain the inherent right to self-defence under Article 51 of the UN Charter when faced with an imminent threat. In any event, state behaviour in cyberspace should be in line with the UN Charter and with the Laws of Armed Conflict. Whether and how states respond to cyber attacks will depend upon the facts of each case, in particular, the extent to which an attack has damaged, or has the potential to damage, vital national interests. In some cases, the proportionate response could simply consist of diplomatic steps taken privately. In other cases, open shaming through the UN Security Council may be appropriate, or even direct punitive steps designed to convince the aggressor to desist from further attacks. A response need not be confined to the cyber realm — in particular, for advanced states heavily reliant on the Internet. For such states to enter into a spiral of potential cyber escalation could leave them worse off than a less-advanced opponent.

In cases of significant damage being done by a cyber attack, action in self-defence could well involve direct military action against those believed responsible (drawing a parallel with precedents in state responses to terrorist attacks). The pursuit of legal redress and indictments may not likely be effective with nations not expected to cooperate in a legal process. In such extreme circumstances, in order to demonstrate their resolve to defend their national interests, states may conclude that they have no alternative but to respond with force against the perpetrators of cyber attacks.

At the end of the day, when deciding whether to publicly attribute culpability for a cyber attack or whether to take direct action, governments need to calculate the costs that would be incurred if they wrongly attribute an attack and consider the potential costs of escalation in that case. There is at present no technical solution to the attribution problem and no easy answer as to how an attacked state should respond.

Offence Prevails in Cyberspace

The present state of digital technology means that those initiating cyber attacks have the advantage over those defending against them. This will likely continue to be the case for the foreseeable future. This is a common characteristic in the history of warfare when innovations (such as the submarine and the tank) are first introduced. In the past, such cases led to the rapid take-up of the new technology by most nations. In the case of cyber attacks and cyber defence, the offensive is dominant to the extent that maintaining state-of-the-art IT security systems is potentially very costly, while launching effective cyber attacks is relatively inexpensive. Offence also trumps defence in the sense that even the best IT security systems in the world can eventually be breached, if the human dimension can be exploited. Therefore, expensive monitoring of networks is needed to identify malware and to detect when attacks or penetrations have occurred. Moreover, since an organization's internal systems will usually be composed of a series of interconnected devices and networks, the side playing defence needs to stop every attack to maintain network integrity. On the other hand, an attacker only needs to breach the

network on one of many attempts to potentially gain access to huge volumes of sensitive data.

New defences may never work perfectly against advanced persistent threats that doggedly target networked systems, but they can effectively increase the cost of undertaking an attack. Making it more expensive to launch cyber attacks can reduce a large proportion of cyber attacks, even if it has little effect upon the most sophisticated and persistent type of cyber attack.

The introduction of robust new technologies such as distributed ledgers, machine learning, quantum computing and the IoT, will more likely than not affect the balance between offence and defence in cyberspace. On the defensive side, distributed ledgers could help preserve data integrity and enhance cybersecurity, thereby making defence against some forms of malicious attacks easier. Adaptive machines that can learn from their past mistakes could improve also cyber defences, making it harder to penetrate a computer network. On the offensive side, quantum computing and the IoT could potentially exacerbate the current situation of offence dominance by alternatively rendering known encryption useless in the face of massive computing power or radically increasing the attack surface available to malicious actors.

Motives versus Ability

Much of the problem with devising effective norms in cyberspace is that low-level attacks get jumbled together with more advanced persistent threats launched by state or state-backed actors. If, as pointed out in the previous section, the general level of digital hygiene was boosted to a sufficient degree to prevent 80 percent or more of cyber attacks, then states would be free to use their cyber resources to counter more advanced persistent threats, making cyberspace more stable and secure.

Until digital hygiene is improved, states need to still be content with a final factor that has contributed to the unruly environment in cyberspace — namely, the decoupling of motive and ability. Now, almost any group or state that wants to launch an attack can do so at an affordable cost — for example, by outsourcing a DDoS attack or development of malware for spear-phishing attacks. This creates a more level playing field between governments, non-state actors and individuals in terms of capabilities than ever before. If nothing else, this symmetry multiplies the number of actors involved in the cyber-security equation, making durable arrangements harder to reach and tougher to preserve.

As a result, cyberspace, as a theatre of conflict between groups and states, is already in play, supported by a combination of technological and political factors, and it is certain to continue.

Why Computer Network Attacks Are Still Uncommon

Cyber attacks, sabotage, espionage, vandalism and disruption in cyberspace continue to proliferate, along with cybercrime. A number of nations have developed offensive cyber capabilities for their military forces for use in support of operations during armed conflict, for example to suppress enemy air defences and radar detection. Some countries, such as the United States and the United Kingdom, have openly declared their intention to have such contingent capability, and presumably more nations are developing it in secret. But many factors have militated against the eruption of a full-blown cyberwar — so far successfully. Cyberwar requires a political motive and must involve the wide-scale use of computer network attacks that do real-world harm and, with a few exceptions, these two factors have so far not aligned on a large scale. There have been individual and relatively isolated incidents of interstate cyber sabotage, mostly to deliver a specific message or warning against the behaviour of the attacked government, but no extensive sustained campaigns of cyber attacks have yet been mounted.

Part of the reason lies in the detailed intelligence and preparation required to mount a series of highly destructive cyber attacks that could penetrate significant elements of critical infrastructure. To design a cyber campaign that puts real pressure on a nation would be a considerable undertaking. Nonetheless, even if we are not likely to soon see a violent conflict, one-off attacks should be expected — either from a state or non-state actor. Sustained campaigns in what is otherwise peace time, would be much harder, and if very serious damage is done, then retaliation must be expected, including the real possibility of a kinetic response. Self-interested concern about escalation has effectively deterred states and groups from doing the damage they might be able to achieve by covert cyber means — so far. To attempt to wage cyberwar is, for advanced nations, equivalent to declaring war by conventional means. So far, no state has felt warranted to go that far.

The absence of cyberwar per se does not mean that cyberspace is not used by governments and non-state actors for malicious purposes. Some governments are known to have either directly used or supported the use of cyberspace as a means to conduct economic espionage and technological disruption, and there is no reason to believe that practice has ended. Countries that are leading innovators are the common target. While all governments spy on each other for political reasons, state-backed economic espionage, which aims to secure an economic advantage for one country's firms, hampers innovation and will ultimately harm global growth.

Almost any group or state that wants to launch an attack can do so at an affordable cost.

Additionally, for some sub-state terrorist groups and rogue states, making daily life difficult for their enemies is already their policy and they have less to lose as they already regard themselves as being in a state of conflict. Sporadic attacks on vulnerable systems and markets are to be expected.

These qualifiers aside, no full-fledged cyberwar has yet taken place. One factor that helps keep a lid on the level of major interstate aggression in cyberspace is a widely shared fear of what might happen if that lid comes off. Uncontrolled escalation could cause an unknown amount of damage. If one attack prompts a retaliatory strike, which, in turn, causes further reaction and escalation, the final price tag is likely to be higher than the attacker wants to pay. No state has yet unleashed the full possibilities inherent in offensive cyber weapons, so it is hard to gauge how much damage could potentially be done to both sides if there was an attempt to engage in full-blown cyberwar.

An additional factor that may limit the use of cyber weapons by advanced states is a growing recognition of the dangers to the attacker of releasing an offensive cyber weapon. The code can be reverse engineered and used to improve the capabilities of the targeted adversary — and of all other potential adversaries, including terrorists and criminals. It is not so much the existence of a "no-first-use" norm as an "only-to-be-used-in-extremis" norm. Another danger exists in this regard. Most developed nations have thus far shied away from the early use of cyber weapons against infrastructure targets or the Internet itself, in part because cyber warfare can be expected to move in unpredictable ways. An offensive cyber weapon could plausibly infect systems that are not directly targeted. Given the interconnected nature of the global Internet, attacks could blowback and potentially infect the attacker as well as the original target.

There is also the danger that once they are used, cyber weapons could inadvertently cause unintended damage to computers and critical infrastructure. This risk is capable of being managed by careful design of the weapon, as in the case of Stuxnet, which infected large numbers of non-targeted machines, but could do no damage to them since it had been designed for

the specific purposes of interfering with the control system of specific nuclear centrifuges. As a general rule, the more malign the effect an attacker wants to obtain, the more specifically the code must be written.

A very different form of damage that cyber weapons can inflict, and is causing increasing concern in many countries, is the capability of an attacker that has penetrated an information system to corrupt databases covertly by manipulating — or spoofing — data. These issues of data integrity can lead to large-scale breakdown of public confidence, wreaking havoc on commerce and politics.

Deterrence cannot be expected to work in cyberspace in the same way it does in the nuclear realm, although there are a few useful parallels. Nuclear deterrence is based on the fact that each side in a conflict between nuclear powers holds at risk vital elements of their opponent's state power. This mutual-risk scenario creates a situation where, if either party used major armed aggression against the other, the attacked party would still have credible options for nuclear use to which the aggressor could not in turn respond, without the certainty of ending up with a wholly unacceptable outcome. Nuclear deterrence is not a system for deterring nuclear use, but of deterring major war of all kinds between nuclear armed states.

There is an element of a sound deterrent posture that can be described as "deterrence by denial" that is sought for gains that cannot be achieved at any acceptable price. In the cyber realm, as described earlier, the costs of an action are likely to outweigh the benefits if the target of the attack retaliates, but the certainty of unacceptable damage that is so important as the backstop for nuclear deterrence is absent in cyber calculations. Retaliation promises retributory damage to an attacker, raising the costs of an action and making it less likely. Terrorist groups or attackers with less sophisticated infrastructure likely will not be deterred in the same way.

Furthermore, if a country has a highly effective defensive system of digital intelligence, monitoring, firewalls and IT security measures, a potential attacker may also be put off, because there is no certainty of a cyber campaign succeeding in wreaking the sought-for damage in the timetable set for the aggression. The aggressor state risks having tipped its hand, and thus will be engaged in an armed conflict with a state whose capabilities to respond remain largely undiminished. This could be called "deterrence by denial."

Deterrence by denial relates to the need for states (and companies for that matter) to re-conceptualize the occurrence of cyber attacks as something akin to getting the common cold or some other virus. For people, being healthy does not mean being forever free from disease. It means being able to bounce back from being ill quickly. In other words, being healthy means being resilient. States need to focus on increasing their resilience to cyber attacks so that once the inevitable happens — a cyber attacks is able to get through — government organizations and critical infrastructure operators are able to identify the problem, contain or remove the pathogen, and return to good health without any lasting adverse consequences.

Deterrence can also be strengthened via "deterrence by taboo." To the extent that the source of a cyber attack can be identified, that actor can be shamed and ostracized if there is a taboo against using cyber weapons to attack the computer networks of others. An analogous form of deterrence is found in the norms surrounding the use of chemical and biological weapons during warfare. Right now, deterrence by taboo remains weak, since attribution is difficult and there are not clear norms against using cyber weapons. Over time, should international efforts at building a baseline norm against the idea that cyber attacks are legitimate come to fruition, deterrence by taboo will be strengthened.

Perhaps most tellingly, deterrence is strengthened by mutual economic interdependence or entanglement. Two countries that are enmeshed economically, financially and especially digitally, will be less likely to target one another because to harm an opponent is to harm oneself. Deterrence does not work perfectly in cyberspace, as in the physical world, but retaliation, denial and mutual vulnerability can all reduce the risk of an aggressor state choosing to start a full-blown cyberwar.

Limiting factors of rational self-interest may help to prevent the eruption of full-blown cyberwar, but they are not sufficient to prevent the growth of unruly behaviour, such as hacks, espionage, sabotage and vandalism online, or the risks of miscalculation, especially if an attacker believes he/she cannot be identified. Such behaviour can never be completely stopped, any more than crime can be abolished, but the risk from malign cyber activity can and must be reduced so that the Internet can continue to be freely used for normal business and social purposes, continue to generate innovation and that confidence in the integrity of the Internet and the digital data it carries can be preserved.

There is a growing convergence around some very clear norms and confidence-building measures for the conduct of states in cyberspace. A good example is in the acceptance of the work of the United Nations Group of Governmental Experts (UNGGE) recommendations on Information Security (A/70/174), and the decision to continue that work. The Commission supports this emerging platform of common practice in establishing a higher level of order in cyberspace, but recommends that more be done.

While the UNGEE report makes good strides by detailing 11 emerging norms, a few stand out as worthy of reiteration in slightly different language, to ensure the widest adoption possible. These emerging norms are useful, but in the borderless world of cyberspace all nations need to work together to prevent the militarization of the Internet and ICT technologies. Other initiatives that have barred the use of cyberspace to conduct economic espionage, such as the bilateral meetings between US President Barack Obama and Chinese President Xi Jinping, could be usefully expanded to include as many nations as possible.

As an increasing percentage of a country's economic and social activity moves online, the potential for more damaging attacks grows. This potential is especially apparent in the area of critical national infrastructure, such as control systems for electricity, gas and water

Recommendation

Mutual resilience enhances stability. Governments, network operators and others who have been dealing with cyber security for longer periods need to assist their counterparts who are just coming online to develop greater resilience to enhance global cyber security.

Recommendation

Deterrence in cyberspace rests on positive entanglement and norms, as well as traditional punishment and denial. Governments seeking lasting cyberpeace should continue to broaden and deepen their mutual economic integration and develop norms that help to reduce the incentive for states to attack one another, whether by cyber or conventional means.

Recommendation

Governments should shift their efforts from trying to develop treaties that limit cyber weapons, as they cannot be verified and flounder on the issue of the indivisibility of offensive and defensive code. Instead, negotiations between governments should focus on agreeing to restrict the list of legitimate targets that can be targeted by cyber attacks.

Recommendation

Consistent with the recognition that parts of the Internet constitute a global public good, the commission urges member states of the United Nations to agree not to use cyber weapons against core infrastructure of the Internet.

grids, nuclear weapons and nuclear power plants, air traffic control systems, health-care systems, satellite systems including Global Navigation Satellite Systems satellite constellations and civilian power grids. Governments, responsible non-state actors and individuals should openly pledge not to target the components of a country's critical infrastructure that are predominately used by civilians.

Recognizing that the global interconnection of devices and economies makes the world's communications and financial systems vulnerable to unintended effects of cyber attacks, governments should publicly acknowledge that they will exercise restraint, avoid destabilizing developments and will apply in cyberspace (as in conventional armed conflict) international humanitarian law and the Geneva Conventions, including the prohibition on attacks on civilian infrastructure. Governments should employ cyber weapons only as a last resort, and then only after having first applied the legal principles of necessity, proportionality and of minimizing the risks of collateral damage.

Cyber attacks do not respect borders or geopolitical jurisdictions. Attributing cyber attacks is difficult and pursuing cyber attackers in other jurisdictions is harder still. Sovereign states are regarded in international law as bearing a responsibility for conventional attacks that originate in their territory, as the Taliban regime in Afghanistan was held responsible for the actions of Osama Bin Laden in 2001. Violation of this norm could be legitimately met with international intervention, including sanctions and resorting to force (in the real world or in cyberspace) in extreme cases. States always retain the right to defend themselves. This right applies to cyber attacks as well as to other forms of armed aggression. If a government, for any reason, is not in a position to prevent attacks from its territory, then it should be regarded as being under an obligation to seek international help to do so.

To assist with the prevention of cyber attacks from within a country's borders, governments should work together and share information freely in order to help with the investigation of cyber attacks in a timely way, allowing investigators from organizations such as Interpol and the computer emergency response team coordination body FIRST access to computers and servers as a part of their investigation. Furthermore, national authorities should, through reform of the MLAT process, be always willing in principle to help with the identification and prosecution of cyber attackers, including serving legal warrants on service providers believed to hold evidence relevant to an investigation.

States also need to build understanding of shared interests in cyberspace if norms of restraint, the identification of vulnerabilities and mutual assistance in the wake of a cyber attack are to effectively emerge. There is currently a trust deficit between the world's major cyber powers. While the recent US-China cyber agreement against economic espionage is a good starting point that has already been endorsed by the G20, there remains a notable trust gap between the United States and China and Russia. Others gaps exist as well. This growing paucity of trust needs to be redressed. States should undertake confidence-building exercises in order to help foster trust between nations. Trust is nurtured by transparency and predictability.

Recommendation

States should work to make it clear who is responsible for responding to cyber attacks within their borders and forge clear linkages between these individuals and their counterparts in other countries. States should also clearly specify how they will respond to cyber attacks, as this will make it clear to others what the consequences of an attack might be.

Improving Multi-stakeholder Internet Governance for the Twenty-first Century

As the influence of the Internet continues to expand, debates about Internet governance have become ever more contentious and the stakes are high.[101] This section highlights three aspects of Internet governance that the Commission believes are vital to address in the short-to-medium term. Their resolution is essential if we are to avoid worsening contention and increasing fragmentation of what has truly become the global nervous system of commerce, communications and social interaction. These three aspects are: the right model for Internet governance institutions and mechanisms; coordination among actors and their activities in the realm of governance; and finding the means to anticipate and address new challenges that are certain to result from Internet-enabled technological change and innovation.

The Right Model for Internet Governance

As the Internet spread rapidly, some world governments questioned whether the bottom-up form of governance originating from its roots in the scientific and engineering community was adequate to deal with the increasingly complex mesh of issues that they thought needed attention. At a very basic level, these are questions of legitimacy: in the sense of requiring the consent of the governed. But there were also questions about whether the governance model truly took into account the necessarily broad range of inputs, and whether the outputs were effective in "achieving the goals that [the governed] care about."[102]

The negotiations leading to the UN WSIS saw the first multilateral negotiation on these issues, and the WSIS process proved to be a defining moment in Internet governance for two reasons. First was the recognition that governments could not negotiate about Internet governance in a vacuum. Accredited civil society representatives (including those from the private sector) who had been invited to attend most of the negotiations as observers, and the expertise they brought to the process, greatly benefited the final result of the summit. The second notable achievement was the development of a definition†† enshrining a role for governments, the private sector and civil society as a widely accepted principle for discussion and negotiation of Internet governance. The WSIS definition has set a bar for legitimacy of any institution or mechanism in the field since that time.

In practice, the principle of multi-stakeholder governance may be honoured as much in the breach as in the observance. In terms of real-world impact, bilateral and multilateral free trade agreements can significantly affect Internet governance issues. Many, such as the Trans-Pacific Partnership Agreement, specifically address important issues such as data localization, encryption, censorship and transparency, all of which are generally regarded as forming part of the Internet governance landscape. However, they are negotiated exclusively by governments and usually in secret. At the same time, such agreements substantially benefit the Internet in a myriad of ways, such as by agreeing on rules to improve competition and market access. Further agreements such as the US-Europe Transatlantic Trade and Investment Partnership and the Trade in Services Agreement under the World Trade Organization are expected to cover similar territory.[103] The fact that these negotiations are open only to governments has inspired protests by non-governmental actors demanding that they be informed and engaged in negotiations to allay fears that the new rules embedded in these agreements favour the interests of governments or corporations over those of other Internet users. The closed nature of the negotiations also means that the benefits governments hope to achieve may not be evident to the general public.

The debate about the most appropriate approach to Internet governance continues to evolve. Until recently, the debate has seen a rough division into three camps: those favouring the continuation of a multi-stakeholder approach that originated organically from entities forming the technical community, as the Internet was created and further developed following commercialization; those favouring a migration to international institutions based, for example, in the United Nations; and a third camp comprising countries favouring a strong governmental model with states exercising sovereign control over their countries' portion of the Internet, accompanied where necessary by international treaties. While these camps continue to have their adherents, recent developments suggest that a fourth model is arising: that of a new and evolving multi-stakeholder approach that involves more conscious deliberation and planning of each stakeholder's respective role. Each of these camps and their respective efforts to achieve an acceptable level of legitimacy are described below.

The Supporters of Continuing the Original Informal, Multi-stakeholder Process for Internet Governance Led by the Technical Community

The legacy Internet governance institutions and mechanisms have primarily technical responsibilities. They involve a broad range of stakeholders whose responsibilities are widely distributed, and whose efforts rely on voluntary cooperation for their effectiveness. These organizations, including the IETF and its institutional home, ISOC, as well as W3C and the Internet Corporation for Assigned Names and Numbers (ICANN), each participated in

†† "A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." (ITU, *WSIS Outcome Documents*, December 2005, paragraph 35, page 75.)

WSIS as observers, and have, to a greater or lesser extent, been the earliest subject of debates about their legitimacy.

Officials from governments and international institutions can find it challenging to participate in traditional Internet standards-setting and policy discussions. Internet governance institutions can sometimes appear to be an exclusive club, not welcoming to newcomers. This perception persists to some extent in today's Internet governance discussions and institutions, and it can discourage the engagement of people used to being involved in traditional government-led institutions and processes. Significant barriers need to be overcome by some would-be participants, especially in their early efforts to engage. To ease the transition, seasoned participants from the technical community may need to adjust their usual blunt approach, understanding the difficulties faced by newcomers and those from different cultures. The institutions themselves need to engage in capacity building and acclimatization to be more welcoming to newcomers.

In an effort to be more inclusive, each of these organizations has developed targeted outreach activities to encourage different stakeholders to understand and, where appropriate, to play an active role in their governance activities. Examples include ISOC's IETF Policy Program, its Next Generation

AN EXAMPLE OF CAPACITY BUILDING AND ACCLIMATIZATION TO INTERNET GOVERNANCE

ISOC has long provided training to help spread the use of the Internet to the world.[104] The Developing Country Workshops were conceived and organized by a number of leading Internet experts beginning with the first workshop at Stanford University in 1993, which was attended by 126 individuals from 67 countries. The workshops provided training on Internet technologies, as well as on operation, management and governance, and most importantly, introduced participants to the international Internet engineering community. These workshops not only helped bring the Internet to many countries in Africa, Asia, the Middle East and Latin America, but they also introduced people to each other, as travel within some regions was difficult. Ultimately, these workshops trained over 1,500 key technologist, industry and government leaders from more than 100 countries.

The most recent evolution of these efforts is ISOC's IETF Policy Program, designed to encourage close interaction between policy experts from developing countries and IETF participants in an environment that supports dialogue, information sharing and problem solving. The program began in 2012. To date, the program has had 128 participants in over 12 different IETF meetings, drawn from 79 different countries, predominantly from Africa, Latin America and the Caribbean, and the Asia Pacific regions.

ISOC also works work with partners to provide training on the full range of Internet topics through an expanded series of programs, and has involved many technologists, network operators and policy/governance experts in these programs, including 289 participants as IETF fellowship recipients, 228 e-learning participants, 138 Internet Governance Forum "Ambassadors," and most recently six participants to take part in OECD meetings through a competitive fellowship program.

Participants in these programs come from across the globe, involving predominantly participants from countries and regions most recently being transformed by the Internet — 173 from Africa, 19 North Americans, 199 from Latin America and the Caribbean, three from the Middle East and North Africa, 199 from Asia and 68 from all parts of Europe.

Leaders Program and Developing Country Workshops; Regional Internet Registries (RIRs) activities such as the regular Roundtable Meetings for Government and Regulators in Europe organized by the Réseaux IP Européens Network Coordination Centre; the W3C programs to support e-government and open data initiatives; and ICANN's Fellowship Program designed to enable participation in ICANN processes by government officials from low, lower-middle and upper-middle economies. Several organizations, notably ICANN and ISOC, have also expanded translation of their key documents into several languages to make their content accessible to wider audiences.

These efforts toward a greater inclusion of other groups have helped the sponsoring organizations to be recognized as having a legitimate role in Internet governance besides the essential standard-setting role, although more needs to be done.

The perception that exclusion on the basis of a lack of familiarity or expertise reduces legitimacy, speaks to one of the two core ways in which legitimacy in Internet governance is produced — namely, via an open process. In traditional standard-setting bodies, the outcome gained its legitimacy not necessarily by being the best alternative or by being the consensus outcome. The standards are accepted by everyone because the process by which they are reached is seen to be open, allowing everyone who wants to the opportunity to provide input into the final product. Having an open process is not the only path to legitimacy, but it is an important component.

Challenges also exist in adapting to new technical models. The technical operation of much of the Internet's infrastructure is accomplished without any direct coordination by a very large number of independent network operators, on the basis of largely voluntary guidelines (with a few notable exceptions that require central coordination, such as names and numbers). Those guidelines are decided upon in a number of different forums. For anyone used to operating in hierarchical governance structures it may be difficult to understand the lack of central authority over the Internet and the lack of national physical boundaries as a means of imposing government policies and laws. Other concepts can equally be challenging, such as accepting the benefits of open standards for Internet software when one is used to promoting and defending proprietary standards to advantage national champions.

Inclusive, open, transparent, bottom-up processes have the benefit of ensuring that no single interest can easily dominate, because the decision-making processes and results are open to anyone interested in reviewing them. This point has often been missed by governments, some of which have been unwilling

Recommendation

All institutions and organizations involved in Internet governance must expand their efforts to identify and reduce institutional barriers to participation by new entrants. Such efforts could include initiatives to sensitize their participants to the challenges of cross-cultural communication, to expand translation of documents, to provide simultaneous interpretation at meetings, to expand outreach efforts and to hold meetings in different regions. At the same time, all organizations with a role in Internet governance, including intergovernmental organizations, trade negotiators, business organizations, not for profits and civil society, should review their governance structures to ensure they are appropriately inclusive.

Recommendation

More governments need to invest effort and resources to build capacity to engage in Internet policy development and implementation. This will be most successful if national governments work together with their private sector representatives, academics, the technical community and civil society to take advantage of their different expertise and experiences in this complex field.

Recommendation

Internet governance institutions should ensure that those affected by Internet governance are aware of where decisions are being made and how they can participate. Information-sharing outreach activities are essential, but so too are educational and capacity-building efforts to teach participants about the technical fundamentals of the Internet that, in many ways, determine what is and what is not possible in policy making. All such efforts should also target young people who make up the first truly digitally literate generation, and who need to understand their responsibility to participate, and the benefits to participating in multi-stakeholder Internet governance, as well as that their involvement will have an influence.

to recognize the value of the long-standing Internet governance mechanisms. It is likely that part of the reason for their opposition has been that participation in organizations such as the IETF was originally from a small group of early adopting and largely Western countries. Opposition based on lack of familiarity has been decreasing as experts from a greater diversity of countries come to participate in the various processes, and as these organizations increasingly engage in outreach through their fellowship programs and through targeted meetings with law enforcement agencies and others. All of these efforts are helping to increase the perception that these multi-stakeholder processes are legitimate.

The key to expanding participation in forums where Internet governance takes place is for governments, businesses and civil society to recognize the importance of the issues, and to understand that the outcomes of these discussions affect everyone, not just the technical community. Governments, business and civil society entities new to non-governmental Internet governance forums can ease their entry by identifying and encouraging those whose training has already prepared them to participate. Initiatives need to be established nationally and regionally to identify individuals or groups in various countries who are willing to learn how to participate both domestically and at the international level, and to create conditions to encourage them. This is particularly important in countries where business and civil society actors are so far not usually engaged in discussions of governance. This is important, because Internet governance processes should be widely inclusive, to ensure that anyone who wants to can have a voice in the decision-making processes that affect them.

A striking characteristic of the Internet environment is that young people are a driving force in finding new ways to use the network, and in the innovation it inspires. However, young people are often not actively involved in Internet governance forums, even though they are directly affected by them. For that reason, it is important that they have opportunities to be exposed to, and be involved in, Internet governance. This will require conscious effort by those involved in the field, particularly to educate young Internet users about broader governance issues and how they can become involved in discussions and decision making about those issues. Generational change will prove a strong force not only for deployment and use of the Internet, but also for expressing the desire and developing the skills needed to participate in decision making about the future of the Internet and how it is governed.

The Supporters of a Mixed Model with a Stronger Role for International Institutions based in the United Nations

As an outcome of the WSIS in 2005, the Internet Governance Forum (IGF) was established under the auspices of the UN Secretary-General as a forum for multi-stakeholder policy dialogue, unencumbered by operational or decision-making responsibilities.[105] Unlike the legacy Internet governance organizations, the IGF — and particularly its Multi-stakeholder Advisory Group — was established as an entity with highly structured formal representation from each of

the stakeholders specified in the WSIS definition.‡‡ This structure has led to on-going debate about what proportion of members each stakeholder group should nominate, from what regions, and how topics are chosen for the annual meetings. Thus, despite its placement within the United Nations, the governance model of the IGF continues to be contested by some of its stakeholders, as might be expected in any community. Nonetheless, the IGF has been recognized as a success, having been renewed for five years in 2010, and for a further 10-year term by the General Assembly's WSIS+10 Review in December 2015. The decision to renew its mandate was, in part, recognition of improvements that have been made, while also recognizing the need for continued evolution in its development, including providing concrete results for its stakeholders.

More broadly, the WSIS+10 Review resulted in an encouraging recognition of the progress made in the first 10 years of cooperation and shared dialogue on Internet governance. The UN General Assembly's endorsement of the WSIS agreement on the importance of the bottom-up, distributed collaborative processes will further encourage the continuing development and spread of the Internet as a force promoting social and economic development and human rights. The unequivocal recommitment to the multi-stakeholder model, the renewal of the IGF mandate and the central focus on creating a digital enabling environment for achieving the UN SDGs show how much progress has been made. While this outcome is to be celebrated, in order to achieve these goals greater stability is required, including finding a stable funding mechanism for the IGF. The Commission supports the continuation of the IGF under the UN Secretary-General, while at the same time recognizing that the IGF cannot progress without an adequate and stable source of funding.

The ITU has been an active arena in the debate about the most appropriate institutional forum for Internet governance, at least since the conclusion of the WSIS (for which the ITU played the leading managerial role).[106] Part of the UN family, it is an intergovernmental agency, although it provides non-voting membership to the private sector, academic institutions and technical organizations that want to contribute to its work. The ITU mandate includes telecommunication standard setting, regulatory advice and powerful roles in the allocation of scarce resources such as the telephone numbering system, satellite orbital slots and radio frequency spectrum. By analogy, some of its member states would prefer a stronger role for the United Nations, and see the ITU as a potential candidate to undertake partial or full management of the parallel responsibilities for the Internet. This has played out in government-only treaty and non-treaty conferences since the post-WSIS Plenipotentiary Conference of 2006. Some member

Recommendation

The United Nations should take practical steps to implement the decision of member states to extend the mandate of the IGF, including providing the necessary funding for its base budget.

Recommendation

All stakeholders should recognize the legitimacy of the multi-stakeholder approach to Internet governance and the critical role played by the Internet technical organizations. Member states of the ITU should explicitly reinforce the complementarity between the ITU's activities and those of the Internet technical organizations, and work with those organizations to avoid duplication and to collaborate where there is the potential to increase benefits.

‡‡ The Multi-stakeholder Advisory Group announced for 2016 comprises 55 members: 19 from governments, 14 civil society, 12 private sector, nine technical community and one from the media. The chair is from a not-for-profit organization. See http://bit.ly/1Th42B0.

states have sought to create authority for the ITU in a number of areas, including Internet numbering (currently the responsibility of RIRs), standard setting (now shared among the IETF, the W3C, the IEEE [Institute of Electrical and Electronics Engineers] and others), charging arrangements for Internet data carriage (for the most part negotiated among private operators), and in a range of other policy areas. Deep divisions on these issues surfaced most forcefully during the 2012 WCIT.[107] The divisions demonstrated there, and the split vote result clearly showed that there is as yet no consensus that moving Internet governance into a UN agency would increase its legitimacy, or its effectiveness.

The Supporters of Favouring a Strong Governmental Model for Internet Governance

The most challenging view of institutional legitimacy in Internet governance comes from countries that favour a strong governmental model with states exercising sovereign control over their countries' Internet, accompanied where necessary by international treaties. Countries in this grouping have not been able to develop much support from other stakeholder groups for this way of doing things, which implies that they are less concerned with establishing their legitimacy with other stakeholders and prefer instead to exert state power to achieve their goals of controlling content online. If this group were to succeed, it is likely that the Internet would fragment into a number of national fiefdoms, with obvious consequences for the existence of a global Internet.

Signs of a New and Evolving Multi-stakeholder Approach for Internet Governance

The results of WSIS+10 are encouraging, but there are other very significant efforts underway that constitute a new phase in the ongoing development of multi-stakeholder Internet governance. The most notable of these was set in motion in 2014, when the US government announced its intention to transition its stewardship of the IANA functions[§§] to the multi-stakeholder community.

The IANA is a key element in how the Internet operates and, since the WSIS, the IANA has been a focus for those who objected to the original governance mechanisms of the Internet. Therefore, the US government announcement was of the greatest possible importance. It also gave rise to a prolonged effort by the broader multi-stakeholder community to meet the requirements set out for the transition. ICANN, as the current IANA functions contractor and the global coordinator for the DNS, was selected as the appropriate party to convene a global multi-stakeholder process to develop the transition plan.[108] The government instructed ICANN to work collaboratively with the directly affected parties, including the IETF, the Internet Architecture Board (IAB), ISOC, the RIRs, top-level domain name operators, VeriSign and other interested global stakeholders to develop a transition plan that would: "support and enhance the multi-stakeholder model; maintain the security, stability, and resiliency of the Internet DNS; meet the needs and expectation of the global customers and partners of the IANA services; and, maintain the openness of the Internet."

[§§] The IANA functions involve the coordination of key technical elements that keep the Internet running smoothly, generally described as: the management of the codes and numbers used in Internet protocols; management of Internet number resources; and management of the root zone of the global DNS. Originally managed by the Information Sciences Institute at the University of Southern California by Jon Postel, these essential functions were contracted to ICANN in 1998 by the US Department of Commerce.

One condition was imposed, stating that the US government "will not accept a proposal that replaces the [US government] role with a government-led or an inter-governmental organization solution."[109] The IANA transition was a test of the efficacy of the multi-stakeholder model.

The multi-stakeholder process established to develop a plan to present to the US government for the IANA transition has proven to be a groundbreaking effort. It may be the first time a multi-stakeholder group much broader than the technical community has been required to come to a joint solution of this importance, including concrete implementation mechanisms, rather than simply to debate the issue. This proved to be a challenge in several ways. Each stakeholder group first had to understand the quite different decision-making mechanisms used by all other stakeholders in the IANA functions, and to build on that understanding to make the multi-stakeholder model work in practical terms. A further beneficial result of the process has been that all stakeholders now share a clear understanding of what are the requirements each client group has of the IANA process, and to find mutually satisfactory approaches to meeting them. The demystification that has resulted will help by grounding discussion of the IANA functions in reality, rather than continuing to look at the function as somehow being at the core of Internet governance itself, as some parties had previously. It should be noted that the ICANN structure includes the Governmental Advisory Committee (GAC), which consists of member national governments and distinct economies recognized in international fora, and observer multinational governmental and treaty organizations (including all the UN agencies with a direct interest in global Internet governance such as the ITU, UN Educational, Scientific and Cultural Organization [UNESCO] and the World Intellectual Property Organization). There are currently 162 GAC members and 35 observers. The GAC actively participated in the stakeholder discussions on the IANA transition.

Those concerned with the numbering- and protocol parameter-related functions were able to finalize their parts of the plan relatively quickly, while the so-called naming community took considerably longer. This likely was because the RIRs and the IETF/IAB/ISOC groups have the longest-established and most explicitly defined relationships with the IANA. In comparison with the naming community, they are also the most homogeneous of the groups.

The naming community, in contrast, comprises a larger group of stakeholders with the greatest diversity, working almost entirely within the ICANN organization. It includes domain name registries, registrars and country code operators, intellectual property lawyers, civil society and human rights activists, corporate users, security experts, technical experts and governments, to name only a few of the interests. Unsurprisingly, there can be considerable divergence among and between the various stakeholders, and they are accustomed to a sometimes contentious way of working toward a solution which is then proposed to the ICANN board of directors to be ratified, rejected or sent back for further work. Because ICANN convened, but was instructed not to control the development of the proposals for the IANA transition, the stakeholders in the naming community were required to achieve an agreement working on their own, and this resulted in a longer process. Many issues had to be resolved. Some governments seized upon the process to seek a stronger role to enable them to approve or reject ICANN decisions. Other powerful interests have opposed the transition altogether, fearing the consequences of the US government "giving up control of the Internet." Many stakeholders expressed serious concerns about the accountability of the ICANN board and staff, leading to the creation of a separate and at least equally difficult process to find new mechanisms to address that very different set of issues.[110]

The long and complex process has produced several important results. All the stakeholders had to learn about the others' working methods, which gave rise to much greater understanding of the problems each faces. The client groups then had to understand their differing relations to the IANA, and to find ways to accommodate all of their needs without infringing on the needs of others. The decisions also had to be workable once they are implemented and become binding after the transition. The rigor imposed by the process gave rise to an increased maturity and responsibility in the ICANN/IANA environment. Importantly, despite this long and sometimes chaotic process, the final result was

Recommendation

The GCIG commends the international Internet community for successfully rising to the challenge of developing a workable proposal for the transition of the IANA function to the global multi-stakeholder community. The Commission urges the US Congress and the US government to accept the transition plan forwarded to them on March 10, 2016.

an acceptable set of proposals that has been sent on to the US government to be implemented. Leaving aside the challenges of achieving that end in an environment strongly affected by the US political system, and complicated by a national election, achieving agreement was a victory. One of the results is a new sense of legitimacy that arises from the process itself. It has shown that in Internet governance, success comes in part from full engagement in the multi-stakeholder processes, even in the face of initial disagreement and differences in the internal workings of each stakeholder group.

This is a sign of a new and evolving multi-stakeholder approach for Internet governance. In developing the IANA transition proposal, some groups were fundamentally representational, such as the governments participating through the GAC, some are entities with clear functional responsibilities, such as the RIRs and the IAB, and some are self-organizing interest groups, such as the various constituencies of the different supporting organizations and advisory councils. Yet each was required to find a way to collaborate in a complex, multi-layered process, and each succeeded.

The strength of this new model is in its adaptability. This model must be recognized and used as a template for the future of Internet governance in a rapidly changing world.

Coordination of Internet Governance

Many players are active in many forums concerned with the rules governing the Internet and its uses. There are many national policy initiatives in place to take advantage of the positive aspects of the Internet while mitigating its more negative impacts. Intergovernmental and international organizations also seek to develop collective approaches to the transnational impacts of the Internet. For example, the OECD has been dealing with fundamental issues such as privacy and transborder data flows since 1980, and continues to be an influential leader in all policy areas that underpin the digital economy. The IGF is active as a discussion forum, and has the potential to provide more concrete guidance through initiatives such as its best practices forums. There also are many other governmental and intergovernmental forums working on a wide range of new challenges (such as spam and cybercrime) and opportunities (such as bridging the digital divide). Non-government actors are also active, including in select international organizations such as the OECD, UNESCO and the ITU; in multi-stakeholder organizations such as the IGF and ICANN; independently through groups such as the Electronic Frontier Foundation, ISOC, and the Association for Progressive Communications; and in academic institutions, such as the Centers for the Internet and Society at Harvard and Keio Universities or the Oxford Internet Institute, to name only a few.

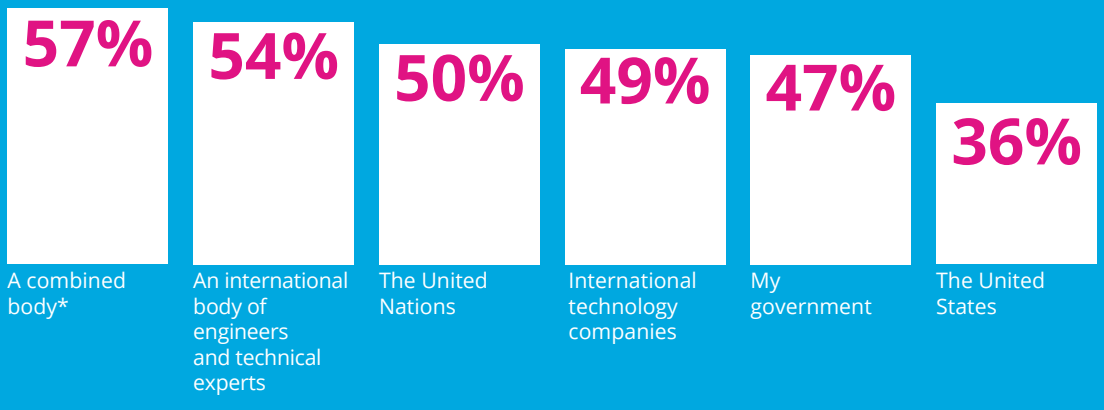
The diversity of these players and their activities shows that all segments of society are trying to come to terms with the opportunities and challenges presented by the Internet, but the sheer number of activities creates its own problems. Those who find themselves involved with these new issues can sometimes be uncomfortable working with new partners and in this new, highly diverse environment. The technical community is used to its work being based on participants' demonstrated expertise, but it is not accustomed to having its work discussed in a politicized environment. Businesses are troubled when concerned citizens and governments seem to increasingly question the effects of new Internet-based

service offerings. Civil society actors, accustomed to the tradition of open debate and decision making in their own organizations, can be uncomfortably insistent that they deserve to engage in governance debates with all partners on an equal footing. All stakeholder groups are finding they are being asked to recognize the legitimacy of the demands made by others, and to adapt. This can require a major perceptual and behavioural shift.

In short, Internet governance is difficult, and all stakeholders are struggling to come to terms with its complexity. Countries and stakeholders that are new to Internet governance, especially at an international level, face the challenge that the Internet governance ecosystem is difficult to grasp due to the multitude of conferences, discussion forums and different Internet governance topics. Significant skills barriers are encountered by various would-be participants, especially in their earliest experiences. Very significant financial barriers also limit participation, due to the large and ever-increasing number of Internet governance meetings held in all parts of the world. Added to these challenges is a degree of confusion arising from a lack of clarity about which participants should, or must, participate in what parts of the multi-stakeholder process. As Mark Raymond and Laura DeNardis point out, it is not necessarily best for all groups to participate in all forums: "some policy making tasks may appropriately be relegated to the private sector, some the purview of traditional sovereign state governance or international treaty negotiations, and some more appropriately multi-stakeholder."[111] This likely will only be sorted out over time, as experience is gained; in the meantime, all stakeholders face the challenge of tracking their issues across a multitude of forums.

While many traditional forums continue to be active platforms for debate, some new purpose-built forums are arising in an effort to help with the problem. One good example has been the NETmundial Global Multistakeholder Meeting on the Future of Internet Governance, held in Sao Paulo, Brazil, in 2014. Nearly 1,500 people from all sectors of society — government (including ministers and high-level officials), industry, civil society and the technical community engaged with one another on an equal footing to hammer out a set of principles for Internet governance, and a road map for the future of Internet governance. Unanimity was not achieved, but the NETmundial outcomes mark a major step by all stakeholder groups toward agreement on the basics of Internet governance, including agreement that Internet governance should be carried out through a distributed, decentralized and multi-stakeholder

Figure 12: How Much Do You Trust Each of the Following to Play an Important Role in Running the Internet?



* A combined body of technology companies, engineers, non-governmental organizations and institutions that represent the interests and will of ordinary citizens, and governments.

Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey.[112]

Recommendation
Coordination should be built around issues, not institutions, and should encourage expert participation.

Recommendation
The Commission is aware of and supports the NETmundial Solutions Map and recommends that permanent resources be allocated to continuing this effort.

ecosystem. This view is confirmed by the recent CIGI-Ipsos poll that showed 57 percent of people want a combined body of governments, private companies, technologists and civil society groups to have a hand in how the Internet is run. This number far outpaces the number of people who support the idea that their government alone (47 percent) should be in charge of the levers of power, as is being advanced by governments that want to impose sovereignty on cyberspace (see Figure 12). This is a positive outcome, but in a field that is already very broad, coordination itself has become a major issue.

Moving forward, it becomes increasingly important to find effective mechanisms to map, understand and, ultimately, coordinate the wide range of national, regional and international efforts to deal with the regime complex surrounding Internet governance. Continuing to address Internet governance in subject-area silos, where stakeholders are often unaware of one anothers' activities, but independently developing and implementing policy, with ad hoc efforts to coordinate related activities, would be a serious mistake. Continuing in this uncoordinated manner is likely to increase the probability of dysfunction or fragmentation. It also would be a major missed opportunity.[113]

There is an urgent need to create a lightweight yet effective mechanism to coordinate and encourage cooperation across institutions and actors in the field of Internet governance. This coordination mechanism must necessarily be tied to existing institutions and processes, but should not result in the creation of a new institution to do the work. The mechanism should be consistent with the 2014 NETmundial principles for Internet governance and build on the Internet's architecture to ensure the public has access to open and available data about decision-making processes, governance practices, issues and responses to enable their participation. The engaged public should have the ability to track work being done and contribute over time. The NETmundial Solutions Map, created by the Governance Lab at New York University and Second Rise, is one approach to facilitate coordination, offering an interactive tool that creates a repository of information that links issues, actors, solutions and resources, and help users understand the current landscape of Internet governance.[114] Another suggestion worth considering is suggested by Nick Ashton-Hart in GCIG Paper No. 12,[115] which advocates using existing forums to coordinate at the institutional level so as to deliver better policy results within existing processes and mandates. Such an approach would especially benefit developing countries by helping them to better decide where to focus their limited resources.

Anticipating and Addressing Upcoming Challenges

Throughout history, changes in technology have sparked new ways of organizing social, economic and political life. The Austrian economist Joseph Schumpeter captures these effects in the phrase "the gale of creative destruction."[116] In the past, technological changes have seemed sudden and disruptive. Yet most pale in comparison to the scope and especially the pace of changes launched by emerging digital technologies. The full ramifications of the shared economy, the IoT and distributed ledgers are hard to fathom from this early vantage point. The one constant of the new normal is constant change.

Rapid disruptions also present significant governance challenges for those who participate in Internet governance institutions and mechanisms. Unsettling disruptions to governments and to foundational businesses have taken place in large part because many countries and industries were not fully aware of the emergence of the Internet, did not foresee the magnitude and scale of the impact Internet technologies would have, and thus were unprepared to react to the emerging threats and opportunities they faced. Of course many of these innovations and their impacts have been positive, even if disruptive; therefore, for the health and stability of economies and societies, it is critical that countries take steps to anticipate change and adapt to innovation.

The impact of new technologies and applications are continuously being felt throughout our economies and our societies. These may best be dealt with by developing and applying shared principles, norms, rules and decision-making procedures — in short, through Internet governance. The rise of the "sharing economy" (Uber, Airbnb) and the early manifestations of the IoT, as well as the innovation of bitcoin and other distributed ledger (blockchain) systems, suggest that these may have even more disruptive effects than we have seen so far. However, attempting to deal with these on an ad hoc, country-by-country basis is not optimal, and particularly not when governments try to cope in isolation. Three examples help to illustrate the challenge.

The Sharing Economy

The disruptions resulting from the rapid spread of the sharing economy are already being felt. Uber has mounted unforeseen challenges to the taxi industry around the world. In New York, the value of taxi licenses (medallions) began to decrease within a few years of Uber's launch. Airbnb is acknowledged to be driving down the growth and the value of the high-fixed-cost hotel industry. Internet-supported, software as a service (SaaS) platform businesses such as these, empower many smaller asset holders, such as car owners, apartment owners and others to compete without having to create *de novo* a new industry to be successful. They only need to attract sufficient customers or partners with assets that are not fully utilized, such as a car in the case of Uber, or motorcycles in the case of GoJek, to make the business model of existing large asset-owning businesses unsustainable. The economic impact is that a single SaaS business can drive a slowdown in many high-fixed-cost sectors across the world. The effects we have seen so far are only the beginning: a few areas likely to reach sufficient scale to suddenly surprise policy makers include peer-to-peer lending, the minute-by-minute reselling of purchased or leased cloud capacity, bicycle and automotive sharing (not just by companies such as Zip or Smove, but between individual owners) — all of which are experiencing early successes. These should be seen as examples of the creative destruction of capitalism, and in the long run are likely to bring considerable value to the economy.

Such developments do raise important governance questions, not least of which are whether there is a need to put a more thoughtful and coordinated shared policy framework in place to deal with the next globalizing, sharing economy disruptions; what are the implications for cross-border tax regimes; and how best to deal with the uncertainty created for employment in traditional jobs and traditional industries. There also is the open question of whether new regulatory requirements should be put in place to protect the public, including requirements for liability insurance. All stakeholders can benefit from shared efforts at gathering data, improving measurement by statistical agencies and collecting information on policy and regulatory approaches in different countries. Hopefully, these and similar efforts can help to answer some of the questions being posed about "who gets what jobs," and the future of our economies.

The sharing economy presents a wide variety of governance challenges, most of which are not immediately part of the Internet governance landscape as generally conceived; however, as experience teaches us, it seems probable that Internet governance questions will inevitably arise as such a disruptive application becomes commonplace. The nature of the challenges we can see already tell us that a much wider range of stakeholders will need to be involved

Recommendation

All levels of government (national, subnational, local), industry, civil society and the technical community, need to be engaged on the new regulatory challenges posed by the sharing economy.

in policy making, including financial institutions, the insurance industry, consumer protection advocates and agencies, and labour unions, to name a few obvious examples. As an immediate step, academic institutions and organizations such as the OECD are encouraged to strengthen research, data collection and sharing experiences of the impacts of the sharing economy on established industries, employment and local communities.

The IoT

The impacts of the IoT are less well understood today than those of the sharing economy but, as already noted, it will certainly have a dramatic effect on the way we live our lives, on the nature of the Internet and on the economy. Again, this is an area where all stakeholders will be severely challenged by rapid and explosive growth, some of it driven forward without building in essential oversight and safeguards. Not only is the IoT going to be large, its impacts will be diverse. A partial list of known applications includes the following: ingestible sensors for use in health care; computer vision; wearables for many purposes; submersible drones; body scanners for retail; smart buildings; agricultural sensing; food safety; and behaviour-based automobile insurance — and this is only the beginning.

While many of these applications will undeniably have positive impacts, alarms are being raised that developers and those involved in commercialization are treating fundamental requirements as an afterthought, most notably by failing to incorporate privacy protection and security by design. Many in the corporate sector do not think that it is essential to build in security if it would mean slowing the introduction and commercialization of their products. This raises the spectre that we may be facing the real danger of the large-scale redistribution of risks to the public in the name of privatization of the profits. Unless governments put effective measures into place to ensure that the industry builds security in at the outset, it will not happen. The consequence will be less private and national security, and the costs will be shifted to the public individually or collectively through the government. Related risks will arise from the unprecedented collection, storage and indexing of IOsT data, much of which will be even more personal and confidential than the data currently connected about our web activity. With widespread private collection of agricultural, scientific, transactional, machinery and maintenance data, the questions of data sovereignty, the application of data privacy laws, limits on private- and public-sector surveillance all become vastly more complex, and vastly harder to govern in a way that accommodates the needs of all stakeholders across a huge diversity of jurisdictions.

Governance responses will be required, but will be difficult to achieve in a timely and responsible manner. Issues of security and the appropriate management of data are only the beginning, but they must be dealt with. As with the sharing economy, the problems are global and affect all stakeholders.

Recommendation

It is essential that industry actors planning to or already engaged in the deployment of IoT hardware and applications accept responsibility for including data protection, privacy protection and strong security as basic design specifications for their products and services. Civil society organizations, academics and the technical community should engage together with government to raise public awareness of the opportunities and threats created by the emerging IoT, and demand that industry accept its responsibility to protect users who will be consciously or unconsciously affected.

Distributed Ledger Technologies

The final example of governance challenges posed by distributed ledger (blockchain) technologies is perhaps the least well understood of the three. Blockchain's earliest application was to track and verify the exchange of bitcoins, but it has already become influential in a broader range of applications. Importantly, as a way to establish trust through a technology platform, it has the potential to impact the traditional roles of governments and major social institutions such as banks, as well as to provide a reliable anchor to the exchange of data and digital products in ways that have not previously been possible. In short, institutions that traditionally play a trusted third-party role can easily be supplanted by not just transnational, but actually stateless, competitors deploying distributed ledger technologies. In developing economies where the depth of public and private institutions is not great, this could be very dislocating. The impacts are starting to be felt and studied by international banks, but also by governments, such as in the United Kingdom [117] and parliaments.[118]

The simplest way to consider distributed ledger technology is as an open, end-to-end communications protocol, analogous to the IP. Distributed ledgers establish an open value exchange protocol, with "value" being very broadly defined. It can enable the exchange of a vast array of data which people find valuable. Just as IP enables innovation at the edge of the network, use of a distributed ledger enables established businesses and entrepreneurs to devise new platforms for the secure and transparent exchange of value. Anything that can be reflected in an agreement can be supported by these Internet-enabled ledgers. It is a distributed ledger: public, transparent, fast and can be grown or adapted to suit a particular purpose. Distributed ledgers let people who have no particular confidence in each other collaborate without having to go through a neutral central authority. As *The Economist* states, "it is a machine for creating trust."[119] But it is a technology still finding its way.

Distributed ledgers let people who have no particular confidence in each other collaborate without having to go through a neutral central authority.

Government institutions, banks, payment transfer systems, insurers, agricultural agents and owners of intellectual property could all find their trusted third-party roles undermined or replaced outright by borderless competitors. In developing economies where the depth of public and private institutions is not great, this could be very dislocating. Clearly, distributed ledger technologies present a global governance challenge with very broad impacts including for Internet governance, as the Internet is an essential enabler of this new trust mechanism.

Recommendation

Private and government trusted third-party operators in all economies should begin to plan how they can respond effectively to a world where use of distributed ledger technologies becomes increasingly common, and to engage in a dialogue among themselves and with affected stakeholders, including legislators and regulators, as to how to best manage the upcoming dislocation.

Being Prepared for an Uncertain Future

Even though we are collectively on the cusp of the next wave of Internet-enabled disruption, some points can be made with confidence. In the Internet governance context, to be able to survive and thrive, there is an increasing need to share information about new developments that may have implications for Internet governance, to be open to unpredictable change and to learn to adapt. Clearly, the private sector, civil society, the technical community, governments and international institutions each bring to the table their unique sources of information and unique perspectives that can help to understand emerging opportunities and challenges in Internet governance that cannot be dealt with by one interest group alone.

It is vital that countries at all levels of Internet adoption and development participate in this process on as much of an equal footing as possible. Innovations now often originate in regions where one might not have expected to find them in the past. Countries that are not already participating in Internet governance need to join the global dialogue both to ensure their present interests are taken into account, but also to safeguard the interests of future generations.

If the capacity to learn, to prepare and to adapt falls short, countries, economies and societies are in danger of falling behind, while those that adapt quickly will move forward. Complicating this danger is the fact that even within a country, economy or society, some may move dramatically ahead while others fall behind, potentially creating a tiered society. Already we see a pattern developing in many economies in which the majority of users are challenged merely to stay current with the relentless pace of innovation, while leading companies and the more digitally skilled individuals continue to push the boundaries of technology use — and to capture disproportionate economic gains and advantages as a result. This can damage the internal cohesion of a state. Distributed ledger technology also appears likely to increase pressure on the authority of the state to the extent it becomes relied on as a trust anchor or source of stability in times of disruptive change. Instead of trusting our fellow citizens, we may instead turn to business, social or religious networks to provide the basis of trust, or to Internet-based anonymous trust anchors such as those enabled by distributed ledgers. Each of these challenges is real, and each will require an adaptable governance response crafted through the multi-stakeholder approach.

A number of institutions could help to identify and stay ahead of the challenges that all countries, economic sectors, businesses and individuals are likely to face in the next few years. Existing institutions, universities and technical institutes are an obvious place to start. These, along with the many national research and education networks (NRENs) that already exist in many countries, are well positioned to track and understand the meaning of rapidly deploying technologies, and to advise the societies in which they are based on necessary and appropriate governance responses. In addition, they are mandated to educate young people, who are best equipped to lead innovation and adaptation.

Private and public think tanks, national statistical agencies and many international organizations based in the United Nations or others such as the OECD, the Asia-Pacific Economic Corporation and the G20, either have or could develop the expertise to monitor and offer advice on emerging governance challenges within their sphere of competence. Key among these is the ability to define indicators and gather data to allow evidence-based analysis of the impacts of Internet innovation, and Internet governance measures, for society and the global and regional economy.

Civil society and business organizations can play a particularly useful role by drawing on their diverse networks of members and contacts, many of whom are intimately involved in creating change. One can think of examples like the Association for Progressive Communications advocacy on the future of Internet governance, the IETF efforts to find antidotes to pervasive monitoring on the Internet, ISOC's leadership programs and the many private-sector organizations such as the Industrial Internet Consortium, or the IEEE already forecasting and preparing to create and adapt to the next wave of innovation.

A collaborative study of the effects of Internet governance and requirements likely to result from the next wave of Internet-enabled innovation must be undertaken in an inclusive, transparent, bottom-up fashion and widely shared among all stakeholders. Scenario-based methodologies could prove useful in anticipating realistic potential impacts.

Recommendation

Universities, technical institutes and experts involved with NRENs and national statistical agencies should establish initiatives to track and understand the meaning of rapidly deploying technologies and to advise the societies in which they are based on necessary and appropriate governance responses.

Recommendation

International institutions and think tanks should bring together policy makers, regulators, planners, educators, corporate heads, entrepreneurs, technologists and professional bodies to assist in policy development to smoothly and effectively develop cross-sectoral and cross-border responses to governance challenge.

Recommendation

Countries must commit to ensuring that their first digitally literate generations have the tools and the connectivity needed to develop and to help their societies to adapt to the coming changes. Emerging generations of "digital natives" must be empowered to exert their influence effectively in the area of Internet governance at earlier ages than would be the norm in many cultures.

Toward a Social Compact on Internet Governance

All developed economies now have multiple Internet dependencies. As more of the world's people come online and as global reliance on the Internet rises, the vulnerability to disruption increases.

Through our work, the Commission has concluded that there is a need to expand the view of Internet governance by creating a new social compact for the digital age. The complex of institutions and individuals that have created the modern Internet and sought to find workable solutions to problems as they arose have been, and largely continue to be, remarkably successful. And yet, we have been convinced that the threats to the universally available, open and secure Internet continue to mount. This report outlines some of the most pressing challenges — among them the need to connect the unconnected by expanding access and improving accessibility for all; to protect and extend human rights; to increase trust and confidence in the network and those who govern it by enhancing protection for personal privacy, individual safety and network security. We also recognize the urgent need to be ever more inclusive in policy making; to set norms and sometimes limits on/for government and corporate behaviour; to avoid the weaponization of the Internet and the potential for disastrous conflicts; and to prevent fragmentation. As readers of this report will recognize, this is only a partial list of the challenges we face in Internet governance.

The Commission has concluded that developing a new Social Compact for the Digital Society has the greatest potential for success as a way for us to address the kinds of challenges faced by Internet governance. We began to express our belief in the value of pursuing this normative approach in a statement released during our June 2015 meeting in The Hague, now included as the Annex of this report.

The Social Compact for the Digital Society will require a very high level of agreement among governments, private corporations, civil society, the technical community and individuals. Governments can provide leadership, but cannot alone define the content of the social compact. Achieving agreement and acceptance will require the engagement of all stakeholders in the Internet ecosystem. At first, it is unlikely that a universal social compact suitable to all circumstances could, or even should, be the immediate goal. The Internet is used and valued across all cultures and all borders. Significant changes of attitude can sometimes evolve more quickly and more flexibly than could be possible through negotiated treaties or international legal instruments. In time, national approaches may gain recognition as good international practices, and may eventually acquire the status of customary international law. But that is many years away, and the speed of technological change argues for flexibility and innovative solutions.

The social compact will contribute to building a new, expanded model of multi-stakeholder governance. Although we recognize the term "multi-stakeholder" can be contentious, it highlights a fundamental truth about the Internet: every part of the Internet ecosystem affects every other part. Thus, the new social compact is not about "balancing" human rights and privacy against states' interests or against commercial rights. It is about ensuring that a framework exists where each actor understands that they have the responsibility to act not only in their own interest, but also in the interest of the Internet ecosystem as a whole. By definition, the process should result in outcomes that are win-win rather than zero-sum games. Effective security, successful business models and human rights are mutually reinforcing in the long run. All interests must recognize and act on their responsibility for a stable, resilient, adaptable and universal Internet in collaboration with all others, or no one is successful.

In the end, it is in the interest of all stakeholders that the Internet remains trusted as a common global resource: open, affordable, unfettered and available to all as a safe medium for further innovation. Government, business and civil society must work together toward that aim.

Success in this endeavour will require that we collaborate to refresh and extend the model of multi-stakeholderism that has so far empowered the growth of the Internet: to conceive of a new model that embraces greater involvement by those whose lives are affected by governance decisions. This new vision of multi-stakeholderism requires a more collaborative, global and decentralized model of decision making; enhanced coordination and cooperation across institutions and actors; increased interoperability in terms of identifying and describing issues and approaches for resolution throughout the ecosystem; open information sharing and evidence-based decision making; and expertise- or issue-based organization to allow for both localization and scale in problem solving.

We know that Internet innovation will bring millions of new users online, creating new opportunities, new benefits and new threats. This will certainly mean that our present understanding of who needs to be involved in Internet governance needs to expand and change to accommodate new interests and new concerned parties. To continue to be effective, Internet governance will need to be more inclusive and more distributed.

We believe this is all possible to achieve in time to avoid the many worst-case scenarios some have posited for the future of the Internet. But we also believe that achieving this vision is only possible if all stakeholders commit to making this new model a reality, through an iterative consensus-building approach to creating a new Social Compact for the Digital Society. From our diverse geographic and stakeholder backgrounds, the GCIG is committed to achieving success, and we invite you to join in.

Looking to the future, the Commissioners are pleased to have been able to make a positive contribution through our work, represented by this report and its recommendations. Where possible, we have identified specific institutions or groups of stakeholders we believe to be the prime actors in addressing an issue, and made concrete suggestions for the direction of work needed. We recognize that we are not and could not be aware of the vast number of groups, institutions and individuals who are or should be involved in

achieving the results we recommend, and apologize for any errors or omissions in this effort.

As we complete our work, the GCIG is encouraged to hear of efforts underway and plans being made to deal thoughtfully with the key issues of Internet governance. We have certainly identified many important areas requiring more research and more thoughtful deliberation that we were not able to undertake during the life of this Commission, and we hope to be able to engage with the work of others in the future. In particular, we strongly recommend more work is done to understand the reciprocal impacts of the Internet in the geopolitical realm, and to develop norms with the aim of preventing the worst potential impacts of geopolitics for the Internet.

We have found that, by and large, considerations of geopolitics/*realpolitik* are missing from the debate on Internet governance. This should not be about the technological aspects of the Internet, but about what the future is going to look like — about who controls what, who gets what, how and when. It will be about the distribution of power in the political realm. As with the effort we are concluding, this discussion will need to engage all players, including the governments of states pursuing a misguided vision of "Internet sovereignty" — erecting borders in cyberspace and asserting the government's right to impose significant constraints on the free flow of information on the Internet. This will require outreach to new stakeholders not normally involved in these discussions. We are satisfied that in our work we broke new ground on this topic. We found it useful, even revelatory, to look at issues of geopolitics in our very diverse group, but the topic proved far too large for us to look at in a comprehensive way in the time available to us. We would encourage others to pick up this effort by undertaking research and broad discussions directed specifically at geopolitical issues. It is certain that the need is very broad, again encompassing economic, human rights, social and technical implications for inclusion and for the on-going viability of the Internet.

The GCIG believes this work is essential, and we commend it to those who follow our work. At the same time, we reiterate the value of approaching Internet-related issues within the conceptual framework of the global social compact. It is not a world where any one group can unilaterally make and impose decisions, no matter if it is as powerful as the nation-state.

Our Internet, Our Future

In its deliberations, the GCIG has benefited from an extraordinary collaboration among its members, drawn from all stakeholder groups and from around the world. We have examined a wide range of issues and debated vigorously, frankly and in the shared desire to find opportunities to realize the benefits the Internet continues to bring, while addressing the challenges we face.

Like the technology of the Internet and the uses people, firms and institutions find for the Internet, the constellation of stakeholders with an interest in Internet governance will certainly grow. Whatever issues arise and whatever decisions affect the course of technical, economic and social development on the Internet, the mechanisms of Internet governance must be adaptable to remain relevant and effective.

One thing has become very clear from our work together. Choices need to be made, and no choice is itself a choice. It is all about who should have what power to control the future of the Internet. The Internet has fundamentally changed the world and as the next billion and the next billion after that join the global conversation it has enabled, it will continue to change the world. The changes we will see can be fundamentally beneficial, or destructive, perhaps even rolling back the gains that have been made. It is up to us as individuals, as members of civil societies, in our roles in business, in governments and in our communities to determine which direction change will take. In writing this report, the GCIG provides practical advice on the steps everyone needs to take to achieve a positive, creative outcome. The Commissioners intend to do their part, and they invite you to join in the effort.

Notes

Preface

1. Dean, David, Sebastian DiGrande, Dominic Field, Andreas Lundmark, James O'Day, John Pineda and Paul Zwillenberg. 2012. "The Internet Economy in the G-20: The $4.2 Trillion Growth Opportunity." The Connected World Series, March. Boston, MA: Boston Consulting Group. www.bcg.com/documents/file100409.pdf.
2. Manyika, James, Michael Chui, Patrick Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin and Dan Aharon. 2015. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey & Company, June. www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

The Essentials

3. GCIG. 2015. *Toward a Social Compact for Digital Privacy and Security*. CIGI and Chatham House. https://ourinternet.org/publication/toward-a-social-compact-for-digital-privacy-and-security/.

Introduction

4. ITU. 2005. "WSIS Outcome Documents." December, para. 35, p. 75.

A Fine Balance: Promoting a Safe, Open and Secure Internet

5. Bradley, Joseph, Christopher Reberger, Amitabh Dixit and Vishal Gupta. 2013."Internet of Everything: A $4.6 Trillion Public-Sector Opportunity." Cisco White Paper. http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe_public_sector_vas_white%20paper_121913final.pdf.
6. Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. 2015. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute.
7. Manyika, James, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov and Dhruv Dhingra. 2016. "Digital Globalization: The New Era of Global Flows." McKinsey Global Institute, February. www.mckinsey.com/business-functions/mckinsey-digital/our-insights/Digital-globalization-The-new-era-of-global-flows.
8. See www.livinginternet.com/i/ia_rfc_invent.htm.
9. See https://cira.ca/blog/byron-blog/how-internet-works-philosophical-explanation.
10. See http://workspace.unpan.org/sites/Internet/Documents/UNPAN95735.pdf paragraph 2.
11. See https://ourinternet.org/publication/the-regime-complex-for-managing-global-cyber-activities/.
12. Nye Jr., Joseph S. 2014. *The Regime Complex for Managing Global Cyber Activities*. GCIG Paper No. 1. www.ourinternet.org/publication/the-regime-complex-for-managing-global-cyber-activities/.
13. Hathaway, Melissa. 2015. *Connected Choices: How the Internet Is Challenging Sovereign Decisions.* GCIG Paper No. 11. CIGI and Chatham House. https://ourinternet.org/publication/connected-choices-how-the-internet-is-challenging-sovereign-decisions/.
14. Hampson, Fen Osler, and Eric Jardine. 2016. *Look Who's Watching: Surveillance, Treachery and Trust Online.* Waterloo, ON: CIGI Press.
15. Bradshaw, Samantha. 2015. *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*. GCIG Paper No. 23. CIGI and Chatham House. www.ourinternet.org/publication/combatting-cyber-threats/.

Transforming Societies and Economies Through Access

16. UN. 2015. UN Sustainable Development Goals. https://sustainabledevelopment.un.org/sdgs.
17. McKinsey. 2014. "Offline and Falling Behind: Barriers to Internet Adoption." McKinsey.com, September. www.mckinsey.com/industries/high-tech/our-insights/offline-and-falling-behind-barriers-to-internet-adoption.
18. McKinsey Global Institute. 2011. "The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity." McKinsey Global Institute, October.
19. ITU. 2015." ICT Facts and Figures." www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.
20. Sprague, Kara, James Manyika, Bertil Chappuis, Jacques Bughin, Ferry Grijpink, Lohini Moodley, and Kanaka Pattabiraman. 2014. "Offline and Falling Behind: Barriers to Internet Adoption." McKinsey Technology, Media, and Telecom Practice.
21. McKinsey Global Institute. 2013. "Lions Go Digital: The Internet's Transformative Potential in Africa." McKinsey Global Institute, November.
22. McKinsey Global Institute. 2013. "China's E-tail Revolution: Online Shopping as a Catalyst for Growth." McKinsey Global Institute, March.
23. Sprague, Kara, James Manyika, Bertil Chappuis, Jacques Bughin, Ferry Grijpink, Lohini Moodley, and Kanaka Pattabiraman. 2014. "Offline and Falling Behind: Barriers to Internet Adoption." McKinsey Technology, Media, and Telecom Practice.
24. Bello, Pablo and Juan Jung, 2015. *Net Neutrality: Reflections on the Current Debate*. GCIG Paper No. 13. CIGI and Chatham House. www.ourinternet.org/publication/net-neutrality-reflections-on-the-current-debate/.
25. Intel. 2012. "Women and the Web: Bridging the Internet gap and creating new global opportunities in low and middle-income countries." www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf.
26. McKinsey Global Institute. 2015. "The Power of Parity: How Advancing Women's Equality Can Add $12 Trillion to Global Growth," McKinsey Global Institute.
27. ITU. 2014. "Measuring the Information Society." www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf.
28. Ibid.

29. OECD. 2015. "Digital Economy Outlook." www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.
30. ITU. 2014. "Measuring the Information Society." www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf.
31. Ibid.
32. Ibid.
33. Ibid.
34. OECD. 2014. "International Traffic Termination." www.oecd-ilibrary.org/docserver/download/5jz2m5mnlvkc.pdf?expires=1463759979&id=id&accname=guest&checksum=4D9B1748F5DD8525783A3DCCBA85B5CF.
35. McKinsey Global Institute. 2015. "Playing to Win: The New Global Competition for Corporate Profits." McKinsey Global Institute, September.
36. Galperin, Hernán. 2016. *How to Connect the Other Half? Evidence and Policy Insights from Household Surveys in Latin America.* GCIC Paper No. 34. CIGI and Chatham House. www.ourinternet.org.
37. World Health Organization. 2011. "World Health Report on Disability." www.digitalaccessibilitycentre.org/images/documents/World-health-report-on-Disability.pdf.
38. ISOC. 2012. "Internet Accessibility: Internet Use by Persons with Disabilities: Moving Forward." www.internetsociety.org/doc/internet-accessibility-internet-use-persons-disabilities-moving-forward.
39. See www.unhcr.org/537334d0427.html.
40. See www.unrefugees.org/2015/06/a-world-at-war/.
41. See www.unhcr.org.uk/about-us/key-facts-and-figures.html.

Ensuring Human Rights for Digital Citizens

42. Omand, David. 2015. *Understanding Digital Intelligence and the Norms that Might Govern It.* GCIG Paper No. 8. CIGI and Chatham House. https://ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no8.pdf.
43. UN Human Rights Office of the High Commissioner. 2015. "Apple-FBI case could have serious global ramifications for human rights." www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138 (see: A/HRC/29/32, paras 8, 42, 60, for example); and "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8.
44. See https://tools.ietf.org/html/rfc7258.
45. See www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf.
46. See www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
47. Berkman Center for Internet and Society at Harvard University. 2016. "Don't Panic. Making Progress on the 'Going Dark' Debate." https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.
48. Schneider, Bruce. 2014. *Data and Golliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W. W. Norton & Company.
49. Bauer, Matthias, Martina F. Ferracane and Erik van der Marel. 2016. *Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization*. GCIG Paper No. 30. CIGI and Chatham House. www.ourinternet.org/publication/tracing-the-economic-impact-of-regulations-on-the-free-flow-of-data-and-data-localization/.
50. See https://citizenlab.org/2013/12/shedding-light-on-the-surveillance-industry/ and https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/.
51. Livingstone, Sonia, John Carr and Jasmina Byrne. 2015. *One in Three: Internet Governance and Children's Rights.* GCIG Paper No. 22. CIGI and Chatham House. www.ourinternet.org/publication/one-in-three-internet-governance-and-childrens-rights/.
52. Frau-Meigs, Davina and Lee Hibbard. 2016. *Education 3.0 and Internet Governance: A New Global Alliance for Children and Young People's Sustainable Digital Development*. GCIG Paper No. 27. CIGI and Chatham House. www.ourinternet.org/publication/education-30-and-internet-governance-a-new-global-alliance-for-children-and-young-peoples-sustainable-digital-development/.
53. Livingstone, Sonia, John Carr and Jasmina Byrne. 2015. *One in Three: Internet Governance and Children's Rights.* GCIG Paper No. 22. CIGI and Chatham House. www.ourinternet.org/publication/one-in-three-internet-governance-and-childrens-rights/.

The Responsibilities of the Private Sector

54. See www.apc.org/en/pubs/frequently-asked-questions-internet-intermediary-l.
55. McKinsey Global Institute. 2013. "*Open Data: Unlocking Innovation and Performance with Liquid* Information." McKinsey Global Institute, October.
56. McKinsey Global Institute. 2011. "Big Data: The Next Frontier for Innovation, Competition, and Productivity." McKinsey Global Institute, June.
57. See www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
58. Digital Equilibrium Project. 2016. "Advancing the Dialog on Privacy and Security in the Connected World." March. https://nebula.wsimg.com/3e4ae1cf8da3d560ac319cfa8dcfa298?AccessKeyId=B2921D5064AE5D77DC67&disposition=0&alloworigin=1.
59. Kramer, Adam D. I., Jamie E. Guillory, and Jeffrey T. Hancock. 2014. "Experimental evidence of massive-scale emotional contagion through social networks." *Proceedings of the National Academy of Sciences of the United States of America* 111 (24): 8788–790. www.pnas.org/content/111/24/8788.full.
60. McKinsey Global Institute. 2015. "A Labor Market That Works: Connecting Talent With Opportunity in the Digital Age." McKinsey Global Institute, June.
61. Manyika, James, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon. 2015. "The Internet of Things: Mapping the Value Beyond the Hype." McKinsey Global Institute.
62. Taylor, Emily. 2016. *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality*. GCIG Paper No. 24. CIGI and Chatham House. www.ourinternet.org/publication/the-privatization-of-human-rights-illusions-of-consent-automation-and-neutrality/.
63. O'Hara, Kieron, Nigel Shadbolt and Wendy Hall. 2016. *A Pragmatic Approach to the Right to Be Forgotten*. GCIG Paper No. 26. CIGI and Chatham House. www.ourinternet.org/publication/a-pragmatic-approach-to-the-right-to-be-forgotten/.
64. Comninos, Alex. 2012. "The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain." Association for Progressive Communications. www.apc.org/en/node/15649.
65. See www.apc.org/en/pubs/frequently-asked-questions-internet-intermediary-l.

66. Scott, Ben, Stefan Heumann and Jan-Peter Kleinhans. 2015. *Landmark EU and US Net Neutrality Decisions: How Might Pending Decisions Impact Internet Fragmentation?* GCIG Paper No. 18. CIGI and Chatham House. www.ourinternet.org/publication/landmark-eu-and-us-net-neutrality-decisions-how-might-pending-decisions-impact-internet-fragmentation/.
67. See, for example, www.huffingtonpost.ca/2011/12/20/bell-internet-throttling-web_n_1160416.html and www.vice.com/en_ca/read/were-at-a-turning-point-in-canada-for-illegal-downloading-328.

Safeguarding the Stability and Resiliency of the Internet's Core Infrastructure

68. Falstrom, Patrik. 2016. *Market-driven Challenges to Open Internet Standards*. GCIG Paper No. 33. CIGI and Chatham House. www.ourinternet.org/publication/market-driven-challenges-to-open-internet-standards/.
69. ISOC. 2012. "Internet Invariants: What Really Matters." February 3. www.internetsociety.org/internet-invariants-what-really-matters.
70. Yoo, Christopher. 2016. *When Are Two Networks Better than One? Toward a Theory of Optimal Fragmentation*. GCIG Paper No. 37. CIGI and Chatham House.
71. Leslie Daigle. 2015. *On the Nature of the Internet*. GCIG Paper No. 7. CIGI and Chatham House. www.ourinternet.org/publication/on-the-nature-of-the-internet/.
72. DeNardis, Laura. 2016 (forthcoming). "The Destabilization of Internet Governance." *I/S: A Journal of Law and Policy for the Information Society*."
73. Weber, Rolf H. 2014. *Legal Interoperability as a Tool for Combatting Fragmentation*. GCIG Paper No. 4. CIGI and Chatham House. www.ourinternet.org/publication/legal-interoperability-as-a-tool-for-combatting-fragmentation/.
74. de La Chapelle, Betrand and Paul Fehlinger. 2016. *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*. GCIG Paper No. 28. CIGI and Chatham House. www.ourinternet-files.s3.amazonaws.com/publications/gcig_28_web.pdf.
75. Chertoff, Michael and Paul Rosenzweig. 2015. *A Primer on Globally Harmonizing Internet Jurisdiction and Regulations*. GCIG Paper No. 10. CIGI and Chatham House. www.ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no10_0.pdf.
76. Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel and Bert Verschelde. 2014. "The Costs of Data Localisation: Friendly Fire On Economic Recovery." ECIPE Occasional Paper No. 3/2014. www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.
77. DeNardis, Laura. 2014. "Internet Points of Control as Global Governance." In *Organized Chaos: Reimagining the Internet*, edited by Mark Raymond and Gordon Smith. Waterloo, ON: CIGI.
78. See, for example, RFC 3833, "Threat Analysis of the Domain Name System (DNS), August 2004.
79. Kolkman, Olaf. 2016 (forthcoming). GCIG Paper on collaborative security.
80. See www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf.
81. Kaplan, James M. and Kayvayn Rowshankish. 2015. *Addressing the Impact of Data Location Regulation in Financial Services*. GCIG Paper No. 14. CIGI and Chatham House. www.ourinternet.org/publication/addressing-the-impact-of-data-location-regulation-in-financial-services/.
82. Verhulst, Stefaan G., Beth S. Noveck, Jillian Raines and Antony Declercq. 2014. *Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem*. GCIG Paper No. 5. CIGI and Chatham House. www.ourinternet.org/publication/innovations-in-global-governance-toward-a-distributed-governance-ecosystem/.

Reducing Crime in Cyberspace

83. Healey, Jason and Barry Hughes. 2016. "Overcome by Cyber Risks? Economic Benefits and Costs of Alternative CyberFutures." Atlantic Council. http://publications.atlanticcouncil.org/cyberrisks/.
84. Zetter, Kim. 2009. "Senate Panel: 80 Percent of Cyber Attacks Preventable." *Wired*. www.wired.com/2009/11/cyber-attacks-preventable/; and Verizon. 2015. *2015 Data Breach Investigations Report*. http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/.
85. Jardine, Eric. 2015. "A Continuum of Internet-Based Crime: How the Effectiveness of Cybersecurity Policy Varies Across Cybercrime Types." In *Research Handbook on Digital Transformations*, edited by F. Xavier Olleros and Majlinda Zhegu. Northampton, MA: Edward Elgar.
86. Chertoff, Michael and Tobby Simon. 2015. *The Impact of the Dark Web on Internet Governance and Cyber Security*. GCIG Paper No. 6. CIGI and Chatham House. www.ourinternet.org/publication/impact-dark-web-internet-governance-cyber-security/.
87. Jardine, Eric. *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. GCIG Paper No. 21. CIGI and Chatham House. www.ourinternet.org/publication/the-dark-web-dilemma-tor-anonymity-and-online-policing/.
88. Owen, Gareth and Nick Savage. 2015. *The Tor Dark Net*. GCIG Paper No. 20. CIGI and Chatham House. www.ourinternet.org/publication/the-tor-dark-net/.
89. UN Office on Drugs and Crime. 2012. "The Use Of The Internet For Terrorist Purposes." United Nations. www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.
90. Kaspersky Security Bulletin. 2013. http://media.kaspersky.com/pdf/KSB_2013_EN.pdf.
91. Jardine, Eric. 2015. *Global Cyberspace is Safer than you Think: Real Trends in Cybercrime*. GCIG Paper No. 16. CIGI and Chatham House. www.ourinternet-files.s3.amazonaws.com/publications/no-16_Web.pdf.
92. Zetter, Kim. 2009. "Senate Panel: 80 Percent of Cyber Attacks Preventable." *Wired*. www.wired.com/2009/11/cyber-attacks-preventable/.
93. Verizon. 2015. "2015 Data Breach Investigations Report." http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/.
94. ITU. n.d. "The Global Cybersecurity Index." www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.
95. Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle and Francesca Spidalieri. 2015. "The Cyber Readiness Index 2.0." http://belfercenter.hks.harvard.edu/publication/26055/cyber_readiness_index_20.html?breadcrumb=%2Fproject%2F69%2Fcyber_security_project.
96. Cybergreen Initiative. n.d. www.cybergreen.net/.
97. Bradshaw, Samantha. 2015. *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*. GCIG Paper No. 23. CIGI and Chatham House. www.ourinternet.org/publication/combatting-cyber-threats/.
98. Gandalf Group. 2014. "The 36th Quarterly C-Suite Survey: Cyber-Security, Trade Agreements and Foreign Investment." www.gandalfgroup.ca/ downloads/2014/C-Suite%20Presentation%20Q3%20 2014%20Oct%2020%20TC.pdf.
99. Schaake, Marietje and Mathias Vermeulen. 2016. "Towards a value-based European foreign policy to cybersecurity." *Journal of Cyber Policy* 1(1).
100. Gagliardone, Iginio and Nanjira Smbuali. 2015. *Cyber Security and Cyber Resilience in East Africa*. GCIG Paper No. 15. CIGI and Chatham House. www.ourinternet.org/publication/cyber-security-and-cyber-resilience-in-east-africa/.

101. Bradshaw, Samantha, Laura DeNardis, Fen Hampson, Eric Jardine and Mark Raymond. 2015. *The Emergence of Contention in Global Internet Governance.* GCIG Paper No. 17. CIGI and Chatham House. www.ourinternet.org/publication/the-emergence-of-contention-in-global-internet-governance/.
102. Scharpf, F. W. 1997. "Economic integration, democracy and the welfare state." *Journal of European Public Policy* 4 (1): 18–36; and Boedeltje, M., and Cornips, J. 2004. *Input and output legitimacy in interactive governance.* (No. NIG2-01). NIG Annual Work Conference 2004 Rotterdam. http://hdl.handle.net/1765/1750.
103. Aaronson, Susan Ariel. 2016. *The Digital Trade Imbalance and Its Implications for Internet Governance*. GCIG Paper No. 25. CIGI and Chatham House. www.ourinternet.org/publication/the-digital-trade-imbalance-and-its-implications-for-internet-governance/; and Singh, Harsha Vardhana, Ahmed Abdel-Latif and L. Lee Tuthill. 2016. *Governance of International Trade and the Internet: Existing and Evolving Regulatory Systems*. GCIG Paper No. 32. CIGI and Chatham House. www.ourinternet.org/publication/governance-of-international-trade-and-the-internet-existing-and-evolving-regulatory-systems/.
104. ISOC. 1993. "Internet Society Launches Developing Country Workshops." www.internetsociety.org/history-timeline/internet-society-launches-developing-country-workshops.
105. ITU. 2005."WSIS Outcome Documents." December, pages 84-85.
106. UN. 2001. United Nations General Assembly Resolution 56/183, December 21.
107. Mauer, Tim and Robert Morgus. 2014. *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate*. GCIGI Paper No. 2. CIGI and Chatham House. www.ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no2.pdf.
108. See www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.
109. Ibid.
110. Shull, Aaron, Paul Twomey and Christopher S. Yoo. 2014. *Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community*. GCIG Paper No. 3. CIGI and Chatham House. www.ourinternet.org/publication/legal-mechanisms-for-governing-the-transition-of-key-domain-name-functions-to-the-global-multi-stakeholder-community/; and Taylor, Emily. 2015. *ICANN: Bridging the Trust Gap*. GCIG Paper No. 9. CIGI and Chatham House. www.ourinternet.org/publication/icann-bridging-the-trust-gap/.
111. Raymond, Mark and Laura DeNardis. n.d. *Multistakeholderism: anatomy of an inchoate global institution. International Theory*. Available on CJO 2015 doi:10.1017/S1752971915000081.
112. See: www.cigionline.org/internet-survey#combined-body-run-the-internet.
113. Ashton-Hart, Nick. 2015. *Solving the International Internet Policy Coordination Problem*. GCIG Paper No. 12. CIGI and Chatham House. ourinternet.org/publication/solving-the-international-internet-policy-coordination-problem/.
114. See http://thegovlab.org/netmundial-solutions-map-released-for-public-comment/.
115. Ibid.
116. Schumpeter, Joseph A. 1994. [1942]. *Capitalism, Socialism and Democracy*. London: Routledge, 82–83.
117. See www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
118. See www.marietjeschaake.eu/2016/03/blockchain-regulatory-technology-or-technology-to-regulate-2/.
119. *The Economist*. 2015. "The technology behind bitcoin could transform how the economy works." www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

Acronyms

3D	three-dimensional
CIGI	Centre for International Governance Innovation
DDoS	distributed denial of service
DNS	domain name system
DNSSEC	Domain Name System Security Extensions
G20	Group of Twenty
GAC	Governmental Advisory Committee (ICANN)
GCIG	Global Commission on Internet Governance
GNI	gross national income
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT4D	ICT for Development
ICT	information and communication technologies
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISOC	Internet Society
ISPs	Internet service providers
ITU	International Telecommunication Union
IXPs	Internet exchange points
MGI	McKinsey Global Institute
MLAT	mutual legal assistance treaty
NRENs	national research and education networks
OECD	Organisation for Economic Co-operation and Development
RAN	Research Advisory Network
RFC	Request for Comments
RIRs	Regional Internet Registries
SaaS	software as a service
SDGs	Sustainable Development Goals
SMEs	small to medium-sized enterprises
Tor	The Onion Router
UNGGE	United Nations Group of Governmental Experts
UNHCR	United Nations High Commissioner for Refugees
VAT	value-added tax
W3C	World Wide Web Consortium
WCIT	World Conference on International Telecommunications
WSIS	World Summit on the Information Society (UN)

Annex

Toward a Social Compact for Digital Privacy and Security

Statement by the Global Commission on Internet Governance Issued at The Hague, The Netherlands on April 15, 2015.

The Global Commission on Internet Governance (GCIG) was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. In recent deliberations, the Commission discussed the potential for a damaging erosion of trust in the absence of a broad social agreement on norms for digital privacy and security. The Commission considers that, for the Internet to remain a global engine of social and economic progress that reflects the world's cultural diversity, confidence must be restored in the Internet because trust is eroding. The Internet should be open, freely available to all, secure and safe. The Commission thus agrees that all stakeholders must collaborate together to adopt norms for responsible behaviour on the Internet. On the occasion of the April 2015 Global Conference on Cyberspace meeting in The Hague, the Commission calls on the global community to build a new social compact between citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the Internet technical community, with the goal of restoring trust and enhancing confidence in the Internet.

It is now essential that governments, collaborating with all other stakeholders, take steps to build confidence that the right to privacy of all people is respected on the Internet. It is essential at the same time to ensure the rule of law is upheld. The two goals are not exclusive; indeed, they are mutually reinforcing. Individuals and

THE FOLLOWING ARE THE CORE ELEMENTS THAT THE COMMISSION ADVOCATES IN BUILDING THE NEW SOCIAL COMPACT:

- Fundamental human rights, including privacy and personal data protection, must be protected online. Threats to these core human rights should be addressed by governments and other stakeholders acting both within their own jurisdiction and in cooperation.
- Interception of communications, collection, analysis and use of data over the Internet by law enforcement and government intelligence agencies should be for purposes that are openly specified in advance, authorized by law (including international human rights law) and consistent with the principles of necessity and proportionality. Purposes such as gaining political advantage or exercising repression are not legitimate.
- In particular, laws should be publicly accessible, clear, precise, comprehensive and non-discriminatory, openly arrived at and transparent to individuals and businesses. Robust, independent mechanisms should be in place to ensure accountability and respect for rights. Abuses should be amenable to appropriate redress, with access to an effective remedy provided to individuals whose right to privacy has been violated by unlawful or arbitrary surveillance.
- Businesses or other organizations that transmit and store data using the Internet must assume greater responsibility to safeguard that data from illegal intrusion, damage or destruction. Users of paid or so-called "free services" provided on the Internet should know about, and have some choice over, the full range of commercial use on how their data will be deployed, without being excluded from the use of software or services customary for participation in the information age. Such businesses should also demonstrate accountability and provide redress in the case of a security breach.
- There is a need to reverse the erosion of trust in the Internet brought about by the non-transparent market in collecting, centralizing, integrating and analyzing enormous quantities of private information about individuals and enterprises — a kind of private surveillance in the service of "big data," often under the guise of offering a free service.
- Consistent with the United Nations Universal Declaration of Human Rights, communications should be inherently considered private between the intended parties, regardless of communications technology. The role of government should be to strengthen the technology upon which the Internet depends and its use, not to weaken it.
- Governments should not create or require third parties to create "back doors" to access data that would have the effect of weakening the security of the Internet. Efforts by the Internet technical community to incorporate privacy-enhancing solutions in the standards and protocols of the Internet, including end-to-end encryption of data in transit and at rest, should be encouraged.
- Governments, working in collaboration with technologists, businesses and civil society, must help educate their publics in good cyber-security practices. They must also collaborate to enhance the training and development of the software workforce globally, to encourage creation of more secure and stable networks around the world.
- The transborder nature of many significant forms of cyber intrusion curtails the ability of the target state to interdict, investigate and prosecute the individuals or organizations responsible for that intrusion. States should coordinate responses and provide mutual assistance in order to curtail threats, to limit damage and to deter future attacks.

This statement provides the Commission's view of the issues at stake and describes in greater detail the core elements that are essential to achieving a social compact for digital privacy and security.

businesses must be protected both from the misuse of the Internet by terrorists, cyber criminal groups and the overreach of governments and businesses that collect and use private data.

A social compact must be built on a shared commitment by all stakeholders in developed and less-developed countries to take concrete action in their own jurisdictions to build trust and confidence in the Internet. A commitment to the concept of collaborative security and to privacy must replace lengthy and over-politicized negotiations and conferences.

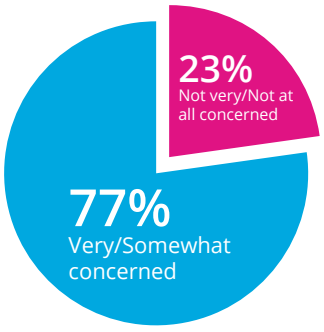
Introduction: The Opportunities and Risks Emerging from the Internet

In a short period of time, the Internet has become enmeshed in our daily lives. Now, people can exchange text, voice, images and data of all kinds — from anywhere in the world, instantly. We can create content, interact digitally, shop internationally with ease, exchange knowledge and ideas, and work together globally. The Internet, as a network of networks, is already capable of communicating and storing almost unimaginable volumes of data online, including data that can be associated with each of us individually and can be used for good or for ill.

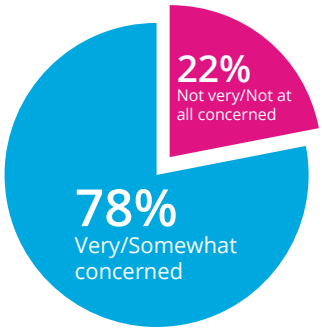
In developed economies, the Internet has already delivered substantial social and economic benefits and is now an essential vehicle for innovation. For the developing world, the Internet can represent a powerful medium for social progress and economic growth, lifting millions of people out of poverty. For those struggling against repressive regimes, it represents a window into the wider world, a voice and a means to mobilize resistance and support. For those wishing to spread violent and hateful ideologies, it represents an unparalleled opportunity to try to radicalize new audiences. For those seeking criminal gains, it represents a way of conducting traditional crimes on a larger scale and conducting new forms of Internet-enabled crime.

It is important to recognize that the communications and data of all of these actors are mixed together in the packet-switched networks and data clouds of the Internet. They all use the same fixed and, increasingly, mobile devices operating with the same Internet protocols. For the authorities charged with tracking down terrorists, countries that conduct espionage, cyber vandals and criminals of all kinds, the Internet provides a reservoir of information about their targets. But at the same time, the ability to access the intermingled data raises concerns over personal privacy and data protection.

Public Concern over Hacking of Personal Accounts



Public Concern over Personal Financial Cybercrime



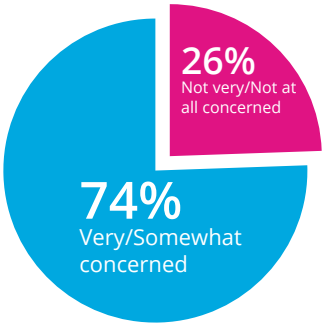
Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey.
Note: The CIGI-Ipsos Global Survey was conducted between October 7, 2014, and November 12, 2014. Twenty-four countries were polled, including Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong, India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, South Africa, South Korea, Sweden, Tunisia, Turkey and the United States. In total, 23,326 Internet users were polled, aged 18–64 in Canada and the United States, aged 16–64 in every other country.

All developed economies now have multiple Internet dependencies. As the global reliance on the Internet rises, the vulnerability to disruption increases. Although Internet access is far from universal, by 2020 the number of Internet users is expected to reach five billion, with each user capable of interacting with any other. The largest portion of this further growth will be in the developing economies. The opportunities to collect, retain and use data for commercial profit, for harm and criminal gain, and for intelligence and security purposes, will increase commensurately. All stakeholders' capacity to protect fundamental human rights and to respond effectively will need to keep pace.

This shift in the availability of personal, commercial and public sector information, and the potential for access to infrastructure and control systems, represents a new source of vulnerability for society, magnified by the growing use of mobile devices and wireless networks that offer additional ways for networks to be penetrated.

These dangers will be accentuated by the advent of the "Internet of Things" that is already starting to connect the key objects and instruments of daily life — our cars, our homes, our appliances, our clothing and much more. In the emerging world of the Internet of Things, everything we do, see, use or touch will leave electronic tracks, enlarging further both the potential commercial and social value of such data. It also will expand the opportunities provided for police and intelligence agencies to learn more about their suspects. Important questions still have to be addressed concerning the vulnerability of such connected systems and the privacy implications of allowing state and private-sector actors to have access to and to share the big data that they will generate. Similarly, there will be a need to clarify that whatever access there is must have a legal basis.

Internet Users' Concern over Private Company Monitoring of Online Activity and Sale of User-generated Data



Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey.

Individuals, Businesses and Governments Face New Challenges

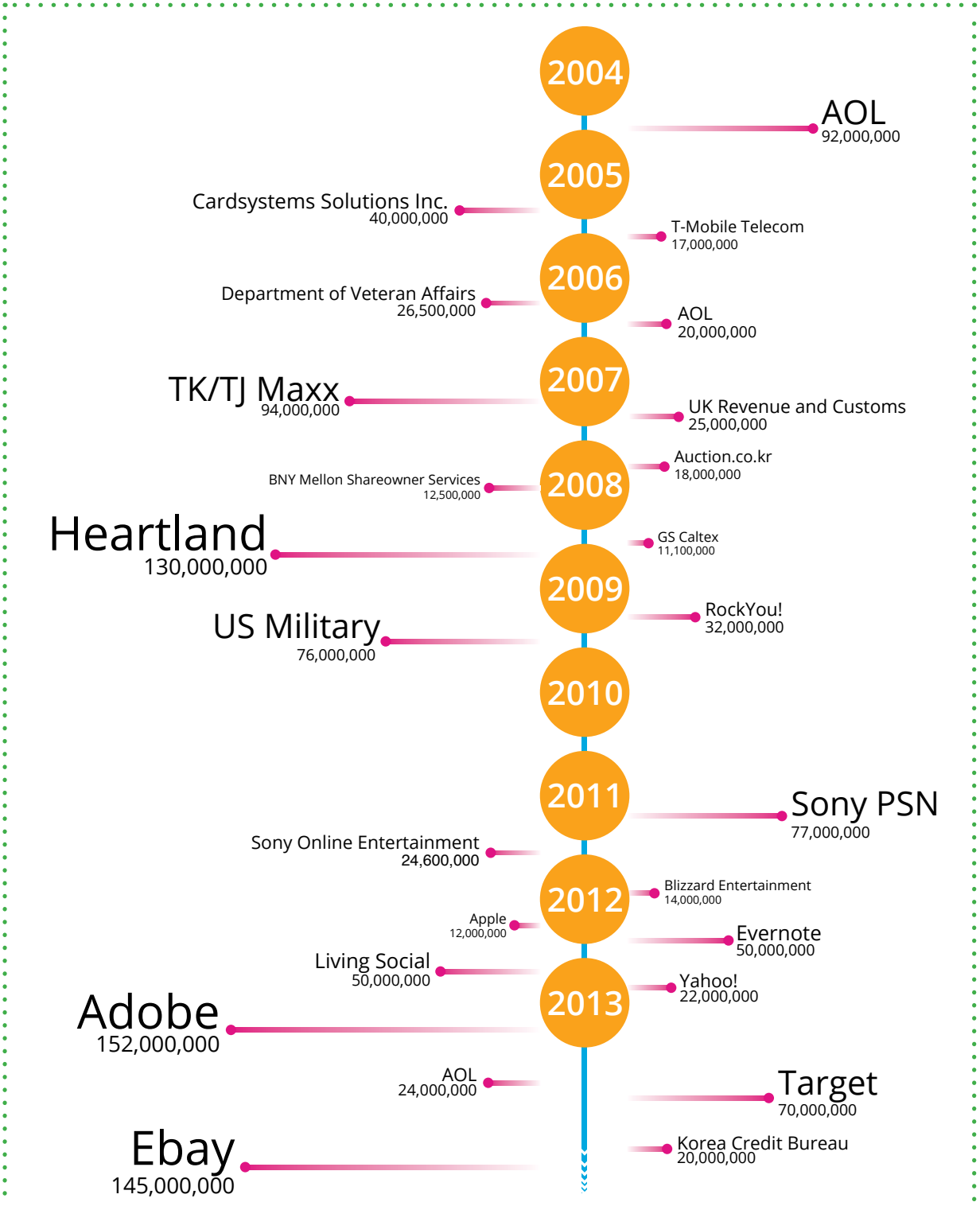
This data revolution has significant and complex negative implications for three sets of actors: individuals, businesses and governments.

A number of surveys indicate that, for individual and corporate users of the Internet, the primary concern is to have adequate assurance of the security of their information against misuse: the cybercrime, vandalism, theft and even terrorist acts that the Internet enables. Not all individuals understand the full scope of what they have placed online deliberately or what information has been captured and stored by others as they go about their daily activities. Nor do most individuals know to what commercial use their data are deployed.

Third parties who have access to data have the potential to monitor, obtain and put to use enormous quantities of private information about individuals and businesses, their communications, their plans, their locations and behaviour, even their shopping, viewing and reading habits. These developments and increasing awareness of them pose a substantial challenge to safety and security, to privacy rights and to citizens' trust in the Internet, which has steadily been eroding. Therefore, these developments are also a substantial threat to the social and economic value of the Internet.

Today, some companies exceed governments in their capacity to collect, store in centralized repositories,

Data Breaches Affecting over 10 Million



Data source: Business Insider. Available at: www.businessinsider.com/data-breaches-infographic-2014-12.

integrate, analyze and make use of personal data. These companies are increasingly attractive targets for cyber intrusion, and susceptible to efforts to jeopardize the confidentiality, availability and integrity of these large data pools. These companies have to demonstrate to their users a high level of respect for, and protection of, the security and privacy of their information. At the same time, companies must exhibit corporate social responsibility in responding to government requests for access to their users' data. They also must contend with increasing requests for access to data from law enforcement overseas due to the transborder nature of many activities taking place on the Internet.

Many companies operating on the Internet also are building their businesses on the use and sale of the data they gather. Often the data are accessed in exchange for providing a free service to their users. Data collected from customers are often used for purposes not explicitly revealed to those who provide the data, and used without their permission. On one hand, this is fuelling data analytics to the benefit of innovation. On the other, it raises concerns about the respect for users' privacy. There is a rising call for regulators, or for the industry itself, to establish standards for transparency and accountability mechanisms to increase confidence in the marketplace.

Governments have the responsibility to pursue Internet policies that are consistent with fundamental human rights and the rule of law, and that promote economic well-being. At the same time, they have a duty to address threats from both state and so-called "non-state actors" such as dictators, insurgents, terrorists and other criminals of all kinds. As data and communications of all types moved from traditional telephone and radio technologies to Internet-based transmission, the opportunities for intelligence agencies to monitor such targets by intercepting and exploiting digital data increased. Yet it is difficult for law enforcement officials to interdict and prosecute transnational criminal activity without having assistance from secret intelligence agencies and their powerful tools of digital intelligence gathering. For example, the pattern and content of messages sent between al-Qaeda, Boko Haram, ISIL (Islamic State of Iraq and the Levant) or other terrorist operatives, and those between members of transnational criminal organizations, would be a high priority for interception by the intelligence and law enforcement agencies of many nations. Cooperation may be required to share specialized resources, because a great deal of criminal and socially damaging activity takes place in the deep recesses of the Internet, including the so-called "dark web." Oversight is required to assure citizens that their rights are not infringed upon in the pursuit of a range of bad actors.

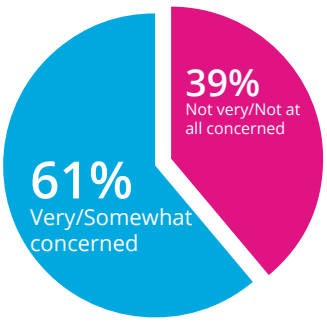
Government activities themselves are vulnerable to terrorists and cyber criminals through the Internet. Many governments are seeking to work with businesses to improve national cyber security to counter the risks of cybercrime, disruption and destruction, especially of critical national infrastructure. These increased risks underscore the importance of governments monitoring threats and attacks online. Nevertheless, some governments are conducting both targeted and mass surveillance in ways that have a chilling effect on fundamental human rights and, in particular, freedom of expression and legitimate dissent and protest, and threatens the realization of the Internet's economic and social benefits.

National and International Responses

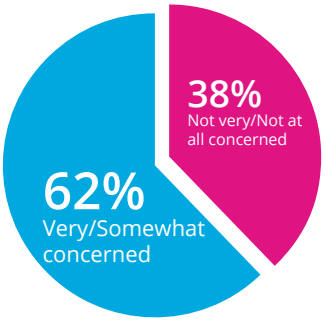
The speed of these contradictory developments in the use of the Internet has left policy lagging behind. Governments struggle to know how to manage the harms the Internet facilitates while preserving its power for good.

At a domestic level, responding to pressure from privacy and civil liberties organizations, in several nations a debate has started about the nature, capacity and legal framework of their digital intelligence activities. Some Internet and telecommunications companies now publish transparency reports about the demands governments place on them. Some nations already have comprehensive legislation to regulate intrusive digital intelligence powers; others do not. Some have parliamentary or judicial oversight (or both) of such activity while some do not have either.

Public Concern over Domestic State Surveillance



Public Concern with Foreign Government Surveillance



Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey.

Personal data protection regulations are mostly not yet suited to the complexity of the digital age — for example, by not adequately regulating the extensive secondary use of personal data or ensuring the transparency of exceptions to privacy for sovereignty and national security purposes. The military utility of offensive cyber operations and intelligence attacks is increasingly recognized, as are the dangers posed by advanced malware and software flaws.

At the international level, all states have subscribed to the UN Universal Declaration on Human Rights, and almost all states have ratified the UN International Covenant on Civil and Political Rights, both of which enshrine the right to privacy in international human rights law. Additionally, some groups of states have usefully developed the right to privacy further, such as in the Convention on Human Rights from the Council of Europe and by implementing the judgments of the European Court of Human Rights. Furthermore, both the NETmundial outcome document and the two recently adopted resolutions from UN General Assembly on the Right to Privacy in the Digital Age affirmed that the same rights that people have offline must also be protected online, including the right to privacy.

The obligation of states to protect and promote rights to privacy and freedom of expression are not optional. Even if they are not absolute rights, limitations to these rights, even those based on national security concerns, must be prescribed by law, guaranteeing that exceptions are both necessary and proportionate. Governments should guarantee the same human rights protection to all individuals within their borders. Clearly, any interference with the right to privacy should not be arbitrary or unlawful, bearing in mind what is reasonable to the pursuance of legitimate aims. The Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines state that exceptions to its principles, including those relating to national sovereignty, national security and public policy (ordre public), should be as few as possible, and made known to the public. The 2013 International Principles on the Application of Human Rights to Communications Surveillance, developed at the initiative of civil society, are an important reference regarding how international human rights law should apply in the current digital environment. States are called to comply with the following principles: legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, safeguards against illegitimate access and the right to effective remedy.

Formal and informal efforts such as these are early steps in the emergence of a new social compact for the digital age.

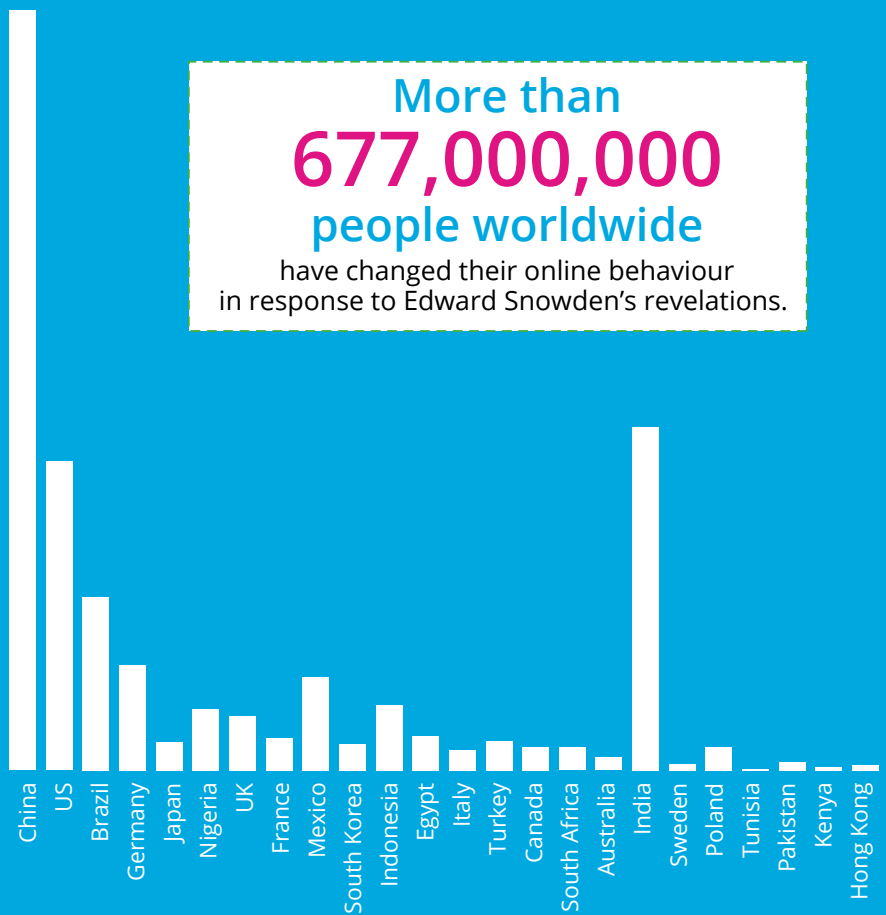
Core Elements of a Social Compact for a Digital Society

There must be a mutual understanding between citizens and their state that the state takes responsibility to keep its citizens safe and secure under the law while, in turn, citizens agree to empower the authorities to carry out that mission, under a clear, accessible legal framework that includes sufficient safeguards and checks and balances against abuses. Business must be assured that the state respects the confidentiality of its data and they must, in turn, provide their customers the assurance that their data is not misused. There is an urgent need to achieve consensus on a social compact for the digital age in all countries. Just how urgent is shown by current levels of concern over allegations of intrusive state-sponsored activities ranging from weakening of encryption to large-scale criminal activity, to digital surveillance, to misuse of personal data and even to damaging cyber attacks and disruption.

In an environment of rapidly changing technologies and social attitudes, a normative approach would be a practical starting point for such an effort. Key elements of a social compact for the digital age will necessarily take different institutional and legal forms in different societies and cultures.

Online Behavioural Change in Response to Edward Snowden's Revelations

More than
677,000,000
people worldwide
have changed their online behaviour
in response to Edward Snowden's revelations.



Data source: CIGI-Ipsos Survey on Internet Security and Trust, available at www.cigionline.org/internet-survey and World Bank Indicators on Population and Internet Penetration Rates, available at http://data.worldbank.org/indicator

Nevertheless, a global social compact should be informed by a number of core elements:

- Fundamental human rights, including privacy and personal data protection, must be protected online. Threats to these core human rights should be addressed by governments and other stakeholders acting both within their own jurisdiction and in cooperation.
- Interception of communications, collection, analysis and use of data over the Internet by law enforcement and government intelligence agencies should be for purposes that are openly specified in advance, authorized by law (including international human rights law) and consistent with the principles of necessity and proportionality. Purposes such as gaining political advantage or exercising repression are not legitimate.
- In particular, laws should be publicly accessible, clear, precise, comprehensive and non-discriminatory, openly arrived at and transparent to individuals and businesses. Robust, independent mechanisms should be in place to ensure accountability and respect for rights. Abuses should be amenable to appropriate redress, with access to an effective remedy provided to individuals whose right to privacy has been violated by unlawful or arbitrary surveillance.
- Businesses or other organizations that transmit and store data using the Internet must assume greater responsibility to safeguard that data from illegal intrusion, damage or destruction. Users of paid or so-called "free services" provided on the Internet should know about, and have some choice over, the full range of commercial use on how their data will be deployed, without being excluded from the use of software or services customary for participation in the information age. Such businesses should also demonstrate accountability and provide redress in the case of a security breach.
- There is a need to reverse the erosion of trust in the Internet brought about by the non-transparent market in collecting, centralizing, integrating and analyzing enormous quantities of private information about individuals and enterprises — a kind of private surveillance in the service of "big data," often under the guise of offering a free service.
- Consistent with the United Nations Universal Declaration of Human Rights, communications should be inherently considered private between the intended parties, regardless of communications technology. The role of government should be to strengthen the technology upon which the Internet depends and its use, not to weaken it.
- Governments should not create or require third parties to create "back doors" to access data that would have the effect of weakening the security of the Internet. Efforts by the Internet technical community to incorporate privacy-enhancing solutions in the standards and protocols of the Internet, including end-to-end encryption of data in transit and at rest, should be encouraged.
- Governments, working in collaboration with technologists, businesses and civil society, must help educate their publics in good cyber-security practices. They must also collaborate to enhance the training and development of the software workforce globally, to encourage creation of more secure and stable networks around the world.
- The transborder nature of many significant forms of cyber intrusion curtails the ability of the target state to interdict, investigate and prosecute the individuals or organizations responsible for that intrusion. States should coordinate responses and provide mutual assistance in order to curtail threats, to limit damage and to deter future attacks.

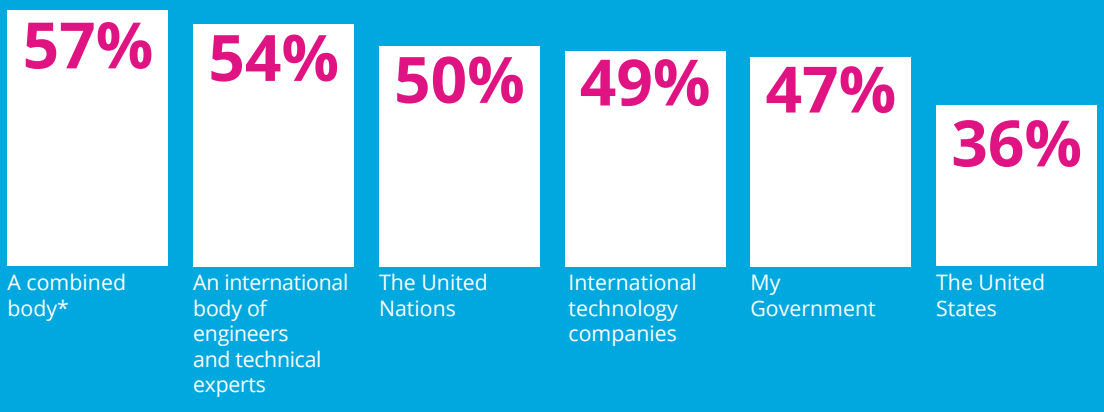
Moving toward a Social Compact for a Digital Society

The social compact for a digital society will require a very high level of agreement among governments, private corporations, individuals and the technical community. Governments can provide leadership, but cannot alone define the content of the social compact. Achieving agreement and acceptance will necessitate the engagement of all stakeholders in the Internet ecosystem. At first, it is unlikely that a universal social compact suitable to all circumstances could, or even should, be the immediate goal. The Internet is used and valued across all cultures and all borders. Significant changes of attitude can sometimes evolve more quickly and more flexibly than could be possible through negotiated treaties or international legal instruments. In the fullness of time, national approaches may gain recognition as good international practices, and may eventually acquire the status of customary international law. But that is many years away, and the speed of technological change argues for flexibility and innovative solutions. The area of secret intelligence is especially difficult to regulate since there is little international law governing it, but even that largely secret domain ought not to be free of ethical and legal considerations.

The social compact will contribute to building a new kind of "collaborative privacy and security." The term highlights a fundamental truth about the Internet: every part of the Internet ecosystem affects every other part. Thus, the new social compact is not about "balancing" human rights and privacy against states' interests or against commercial rights. It is about ensuring that a framework exists where each actor has the responsibility to act not only in their own interest, but also in the interest of the Internet ecosystem as a whole. By definition, the process should result in outcomes that are win-win rather than zero-sum games. Effective security, successful business models and human rights are mutually reinforcing in the long run. All interests must recognize and act on their responsibility for security and privacy on the Internet in collaboration with all others, or no one is successful.

In the end, it is in the interest of all stakeholders that the Internet remains trusted as a common global resource: open, affordable, unfettered and available to all as a safe medium for further innovation. Government, business and civil society must work together toward that aim.

The Public's Preference for Multi-stakeholder Governance



* A combined body of technology companies, engineers, non-governmental organizations and institutions that represent the interests and will of ordinary citizens, and governments

Data source: CIGI-Ipsos Global Survey on Internet Security and Trust. Available at www.cigionline.org/internet-survey

Conclusion

These recommendations are put forward by the Global Commission on Internet Governance to encourage a strong consensus among all stakeholders that the benefits of the Internet for humankind must not be put at risk, whether by disproportionate state behaviour in cyberspace, by criminal activity or by business activity undermining assurance in the confidentiality, integrity and availability of information on the Internet. Advancing a new normative framework, which accounts for the dynamic interplay between national security interests and the needs of law enforcement, while preserving the economic and social value of the Internet, is an important first step to achieving long-term digital trust. The Commission is committed to building on this statement by continuing its program of research and publication, undertaken in collaboration with partners from all sectors.

GCIG Biographies

Carl Bildt, Chair of the GCIG / @carlbildt. Carl Bildt served as Sweden's foreign minister from 2006 to 2014, and was prime minister from 1991 to 1994, when he negotiated Sweden's EU accession. A renowned international diplomat, he served as EU Special Envoy to the former Yugoslavia, High Representative for Bosnia and Herzegovina, UN Special Envoy to the Balkans and Co-Chairman of the Dayton Peace Conference.

Gordon Smith, Deputy Chair of the GCIG / @GordonSmithG20. A former Canadian deputy foreign minister, NATO ambassador and G7/G8 Sherpa, Gordon Smith is a distinguished fellow at CIGI. He has been a key contributor to CIGI's G20 research activities, events and publications; his current work focuses on the convergence of technology and global affairs.

Fen Osler Hampson, Co-Director of the GCIG / @FenHampson. Fen Osler Hampson is a distinguished fellow and director of the Global Security & Politics Program at CIGI. He previously served as director of the Norman Paterson School of International Affairs and is concurrently Chancellor's Professor at Carleton University.

Patricia Lewis, Co-Director of the GCIG / @PatriciaMary. Patricia Lewis is research director of international security at Chatham House. In previous positions, she has been deputy director and scientist-in-residence at the James Martin Center for Nonproliferation Studies, Monterey Institute of International Studies, Middlebury College, and director of the UN Institute for Disarmament Research.

Sultan Sooud Al Qassemi / @SultanAlQassemi. Sultan is a UAE-based commentator on Arab Affairs writing for numerous local and international publications including *The National*, *Gulf News*, ***The New York Times***, *Financial Times*, and the ***Guardian***. He tweets prolifically @SultanAlQassemi and has over 270,000 followers and was listed in the "140 Best Twitter Feeds of 2011" by *Time Magazine*. He is a non-resident fellow at the Mohamed Bin Rashid School of Government in Dubai.

Dominic Barton is the global managing director of McKinsey & Company, a global management consulting firm. He served as McKinsey's chairman in Asia from 2004 to 2009, and led McKinsey's office in Korea from 2000 to 2004. Dominic is an active participant in many international fora, including the World Economic Forum, Le Cercle des Économistes: Les Rencontres Économiques d'Aix-en-Provence, the Asia Business Council, and the China Development Forum.

Pablo Bello / @pablobello. Pablo Bello Arellano is a Chilean economist, expert in telecommunications and economic regulation. Pablo was appointed Secretary General of the Asociación Iberoamericana de Centros de Investigación y Empresas de Telecomunicaciones in June 2011. During the presidency of Michelle Bachelet (2006-2010), he served as Vice-Minister of Telecommunications.

Pascal Cagni is an independent director at Kingfisher and Vivendi. He is a business angel in multiple start-ups of the digital economy. From 2000 to 2012, Pascal led Apple EMEIA (Europe, Middle East, India, Africa) to become the largest and fastest growing region for Apple.

Moez Chakchouk / @mchakchouk. Moez Chakchouk is chairman and CEO of the *Tunisian Post*, and former Chairman and CEO of the Tunisian Internet Agency, the primary Internet service provider in Tunisia. Moez has served as a research engineer at the Centre of Telecommunication Studies and Research, Director of Interconnection and Access at the Telecommunications Regulation Authority and Adviser to the Minister of Communications Technology.

Dae-Whan Chang is chairman of the Maekyung Media Group, which includes the *Maeil Business Newspaper* and Maeil Broadcasting Network. He served as Acting Prime Minister of Korea (2002), chairman of the Korean Association of Newspaper (2005-2010), chairman of the board at Sejong Center for the Performing Arts (2008-2011) and member of the National Competitiveness Council (2008-2013). He serves as board member of World Association of Newspapers and founder and executive chairman of World Knowledge Forum.

Michael Chertoff is chairman and co-founder of the Chertoff Group and senior of counsel, Covington & Burling LLP, was secretary of the US Department of Homeland Security from 2005 to 2009. Previously he was a US Court of Appeals judge and chief of the US Department of Justice Criminal Division.

Dian Triansyah Djani is the director general of America and Europe in Indonesia's Ministry of Foreign Affairs. He was director general for ASEAN Cooperation and drafter of the ASEAN Charter. He was also Ambassador and Permanent Representative of Indonesia to the UN, WTO, ITU, WIPO, WHO, UNCTAD, ILO and other international organizations in Geneva. He served, among others, as President of the UNCTAD's Trade and Development Board.

Anriette Esterhuysen / @anriette. A resident of Johannesburg, South Africa, Anriette Esterhuysen is the executive director of the Association for Progressive Communications, an international network and non-profit organization committed to providing affordable Internet access to all people to enhance social justice and development. She was previously executive director of The Southern African NGO Network (SANGONeT), where she helped establish Internet connectivity in South Africa.

Hartmut Glaser / @hartmutglaser. Hartmut Glaser is executive secretary of the Brazilian Internet Steering Committee and serves on the board of directors of LACNIC. He has served as special adviser to the dean of Escola Politécnica at the University of São Paulo, special adviser to the rector of the University of São Paulo, and special adviser to the president of the Foundation for Research Support of the State of São Paulo.

Dorothy Gordon is the Director-General of Ghana's Advanced Information Technology Institute, the Ghana-India Kofi Annan Centre of Excellence in ICT (AITI-KACE). She is at the vanguard of ICT development in Africa. Under her leadership, AITI-KACE seeks to bring African innovation to African consumers to forge a sustainable industry of communication technology. Dorothy sits on the board of several technology-based organizations.

Angel Gurría joined the OECD as secretary-general in June 2006, following a distinguished career in public service. As Mexico's Minister of Foreign Affairs from December 1994 to January 1998, he made dialogue and consensus-building one of the hallmarks of his approach to global issues. From January 1998 to December 2000, he was Mexico's Minister of Finance and Public Credit. As OECD secretary-general, he has reinforced the OECD's role as a "hub" for global dialogue and debate on economic policy issues while pursuing internal modernization and reform.

Dame Wendy Hall / @DameWendyDBE. Dame Wendy Hall is professor of computer science and executive director of the Web Science Institute at the University of Southampton. One of the first computer scientists to undertake serious research in multimedia and hypermedia, the influence of her work has been significant in many areas including digital libraries, the development of the Semantic Web, and emerging research discipline of Web Science.

Melissa Hathaway is a CIGI distinguished fellow and president of Hathaway Global Strategies LLC. She is also a senior advisor at Harvard Kennedy School's Belfer Center and the Chairman of the Council of Experts for the Global Cyber Security Center in Italy. She served in two US presidential administrations, where she spearheaded the Cyberspace Policy Review for President Barack Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush.

Mathias Müller von Blumencron / @mtblumencron. Journalist Mathias Müller von Blumencron is editor-in-chief digital media at the German newspaper Frankfurter Allgemeine Zeitung. Prior to his current appointment, Mathias was an editor-in-chief of Germany's leading weekly *Der Spiegel*, where he managed all digital products, and editor-in-chief of Spiegel Online, which he built into Germany's most successful and award-winning news site.

Beth Simone Noveck / @bethnoveck. Beth Simone Noveck, founder and director of The Governance Lab, is a visiting professor at New York University's Robert F. Wagner Graduate School of Public Service and the MIT Media Lab. Currently on leave from the Institute for Information Law and Policy at New York Law School, she served in the White House as the first US deputy chief technology officer and is founder of the White House Open Government Initiative.

Joseph S. Nye Jr. / @Joe_Nye. Joseph Nye Jr. is a University Distinguished Service Professor and former dean of the Kennedy School at Harvard University. He has served as assistant secretary of defense for International Security Affairs, chair of the National Intelligence Council, and deputy undersecretary of state for Security Assistance, Science and Technology.

Sir David Omand was the first UK security and intelligence coordinator from 2002 to 2005 as Permanent Secretary in the Cabinet Office. Previously, he was Permanent Secretary of the UK Home Office and Director of GCHQ (the UK Sigint and cyber security agency). He is a Fellow of Corpus Christi College Cambridge and is Senior Independent Director of Babcock International Group PLC.

Nii Quaynor / @niinarkuquaynor. Nii Quaynor is chairman of the board of directors at National Information Technology Agency. He pioneered Internet development and expansion throughout Africa for nearly two decades, establishing some of Africa's first Internet connections and helping set up key organizations, including the African Network Operators Group. He is a member of the IGF Multi-Stakeholder Advisory Group.

Latha Reddy served in the Indian Foreign Service from 1975 to 2011. She was Ambassador of India to Portugal and Thailand and Consul-General in Durban, South Africa. She was Secretary (East) in the Indian Foreign Ministry, overseeing Indian foreign policy in Asia. She also has extensive experience in multilateral and regional diplomacy. She was appointed as the Deputy National Security Advisor and Secretary, National Security Council Secretariat from 2011 to 2013.

Marietje Schaake / @MarietjeSchaake. Marietje Schaake has served as a Member of the European Parliament from the Netherlands since 2009 with the European liberal group (ALDE). She serves on the International Trade committee, the committee on Foreign Affairs, and the subcommittee on Human Rights. She is the founder of the European Parliament Intergroup on the Digital Agenda for Europe. She is Vice-President of the US Delegation and serves on the Iran Delegation.

Tobby Simon is the president of Synergia Foundation, a think tank in India that works closely with industry, polity and academia to establish leading edge practices through applied research in the domains of geopolitics, geoeconomics and geosecurity. He has been an adviser to several international organizations such as the World Health Organization , the European Union and served as the Regional Director for the World Information Technology and Services Alliance.

Michael Spence / @amspence98. Michael Spence is the William R. Berkley Professor in Economics and Business at the Stern School of Business, New York University. He received the Nobel Memorial Prize in Economic Sciences in 2001, and the John Bates Clark Medal from the American Economics Association in 1981. He is a fellow of the American Academy of Arts and Sciences and the Econometric Society.

Paul Twomey / @PaulDTwomey. Paul Twomey was the CEO and president of ICANN from 2003 to 2009. He has held executive positions within the Australian Government's foreign trade organization and has served as CEO of the National Office for the Information Economy. He is former senior consultant with McKinsey & Company. Paul is also the founder of ArgoPacific.

Pindar Wong / @PindarWong. Pindar Wong is the chairman of VeriFi (Hong Kong) Ltd, a discreet Internet financial infrastructure consultancy. He is a Bitcoin protocol enthusiast and chairs ScalingBitcoin.org. Previously, he co-founded Hong Kong's first licensed ISP in 1993, was the first vice-chairman of ICANN, chairman of the Asia Pacific Internet Association, alternate chairman of Asia Pacific Network Information Center and elected trustee of the Internet Society.

Commission Support

Laura DeNardis, Director of Research of the Global Commission on Internet Governance / @LauraDeNardis. A scholar of Internet architecture and governance, Laura is a CIGI senior fellow and professor at American University. She is an affiliated fellow at Yale Law School's Information Society Project and previously served as its executive director.

Acknowledgements

CIGI, Chatham House and the Commissioners of the GCIG would like to thank the many individuals who contributed to and facilitated the work of the Commission including but not limited to our Research Advisory Network, research paper authors and peer reviewers, the many individuals who addressed the Commission and the behind-the-scenes personnel. Below are just a few of the many individuals who contributed to the success of the commission.

Susan Aaronson
Ahmed Abdel-Latif
Sunil Abraham
Marcus Adomey
Izumi Aizu
Eric Akumiah
Vera Akumiah
Teki Akwetey
Virgilio Almeida
Albert Antwi-Boasiako
Papa Arkhurst
Nick Ashton-Hart
Bassem Awad
John Baird
Jim Balsillie
Sukho Bang
Matthias Bauer
Tim Barber
Caroline Baylon
Tammy Bender
Subimal Bhattacharjee
Anne Blayney
Sarah Box
Dan Breznitz
Francisco Brito Cruz
Deborah Brown
Jasmina Byrne
Barry Carin
John Carr
Susan Chalmers
Anupam Chander
Kilnam Chon
David Clark
Jane Coffin
Derrick Cogburn
Jorge Contreras
Aras Coskuntuncel
Chiara Criscuolo
Leslie Daigle
Tony Danker
William Danvers
Primivera De Filippi
Bertrand de la Chapelle
Anthony Declercq
Ronald Deibert
Oleg Demidov
Kevin Dias
Danilo Doneda
Bill Dutton
Olof Ehrenkrona
Laurent Elder
Ben Eshun
Patrik Faltstrom
Paul Fehlinger
Martina F. Ferracane
Nathalia Foditsch
Benedicto Fonseca
Liesyl Franz
Divina Frau-Meigs
Lynn Fullerton
Iginio Gagliardone
Helani Galpaya
Hernan Galperin
Urs Gasser
Alison Gilwald
Alexia Gonzalez-Fanfalone
Jennifer Goyder
Andrea Hackl
Joseph Lorenzo Hall
Yousef Hamidaddin
John Hay
Lisa A. Hayes
Jerome Henique
Archie Hesse
Stefan Heumann
Lee Hibbard
Kaili Hilkewich
Jeanette Hoffman
Patricia Holmes
Joi Ito
Merit Janow
Daniel Jean
Michael Jenson
Yoon Jong-Rok
Juan Jung
Brian Kahin
James Kaplan
Olga Khrustaleva
Burcu Kilic
Matthieu Kimmell

Olaf Kolkman
Konstantinos Komaitis
Johanna Kruger
Fred Kuntz
Nicole Langlois
Young-eum Lee
Ronaldo Lemos
Nanette Levinson
Jacqueline Lipton
Sonia Livingstone
Emma Llanso
Susan Lund
Ambassador Kenneth Macartney
Rebecca Mackinnon
Yahya Majali
Aaron Martin
Meryem Marzouki
Tim Maurer
Rohinton P. Medhora
Pamela Miller
James Moore
Sara Moore
Robert Morgus
Vivian Moser
Dora Mountain
Michael Murphee
Robin Niblett
Kieron O'Hara
Gareth Owen
Sam Paltridge
Lorrayne Porciuncula
Jillian Raines
Mark Raymond
Fernanda Ribeiro Rosa
Uri Rosenthal
Paul Rosenzweig
Carolina Rossini
Kayvaun Rowshankish
Nanjira Sambuli
Tatevik Sargsyan
Nick Savage
Lynn Schellenberg
Ben Scott
Kristen Scott Ndiaye
Eric Sears
Nigel Shadbolt
Her Excellency, Minister of ICT Majd Shweikeh
Harsha Singh
Lee Sir-Goo
Ambassador Per Sjogren
Steve Song
David Souter
Vincenzo Spieza
Susan Stone
Eli Sugarman
Emily Taylor
High Commissioner Christopher Thornley
Spencer Tripp
Som Tsoi
Rudolph van der Berg
Erik van der Marel
Stephan Verhulst
Mathias Vermeulen
Melodie Wakefield
Michael Walma
Verena Weber
Rolf Weber
Jeremy West
Carl Fredrick Wettermark
Hong Won-Pyo
Bill Woodcock
Christopher Yoo
Sean Zohar

Sponsors

CIGI, Chatham House and the Commissioners of the GCIG would like to recognize and thank the following sponsors for their generous support, which facilitated the work of the GCIG on one of the most pressing global public policy issues of our time, Internet governance:

Canadian Copyright Corporation

Government of Canada

Government of Jordan

Government of the Netherlands

Government of Sweden

Government of the United Kingdom, Foreign and Commonwealth Office

His Excellency Sheikh Sultan Al Qassemi

International Development Research Centre

Kakao Corporation

The John D. and Catherine T. MacArthur Foundation

Maekyung Media Group

McKinsey & Company

Ministry of Research and Innovation of the Province of Ontario

Oasis500

Organisation for Economic Co-operation and Development

Synergia Foundation

The Annenberg Retreat at Sunnylands

The Royal Patronage of HH the Crown Prince of Jordan

The Global Commission on Internet Governance and its supporting Research Advisory Network is comprised of independent academics and practitioners. The views expressed herein are those of the members of the Global Commission, and where applicable of individual authors, and do not necessarily reflect the views of CIGI, Chatham House or any sponsoring organizations.

About CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

About Chatham House

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI Masthead

Executive

President	Rohinton P. Medhora
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Chief of Staff and General Counsel	Aaron Shull
Director of Communications and Digital Media	Spencer Tripp

Publications

Publisher	Carol Bonnett
Senior Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Kristen Scott Ndiaye
Publications Editor	Lynn Schellenberg
Graphic Designer	Sara Moore
Graphic Designer	Melodie Wakefield

Communications

For media enquiries, please contact communications@cigionline.org.

Global Commission on Internet Governance

ourinternet.org

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444
fax +1 519 885 5450
cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE,
United Kingdom
tel +44 (0)20 7957 5700
fax +44 (0)20 7957 5710
chathamhouse.org