Global Commission on Internet Governance

The Essentials

CIGI

CHATHAM HOUSE
The Royal Institute of
International Affairs

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

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

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.

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

Introduction

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 US$4.2 trillion in 2016. The Internet of Things (IoT) could result in upwards of $11.1 trillion in economic growth and efficiency gains by 2025. 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.

A global Research Advisory Network (RAN) supported the Commission, producing more than 50 research papers on topics including Internet fragmentation, human rights, interconnection and 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 the final 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 Commission presents their final report — *One Internet* — 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 following Essentials is an excerpt from the GCIG final report, *One Internet*. **The full report and all of the GCIG's research papers are available for download free of charge at www.ourinternet.org**.

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 Internet of Things (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 US$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 US$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 US$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 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.

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 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?

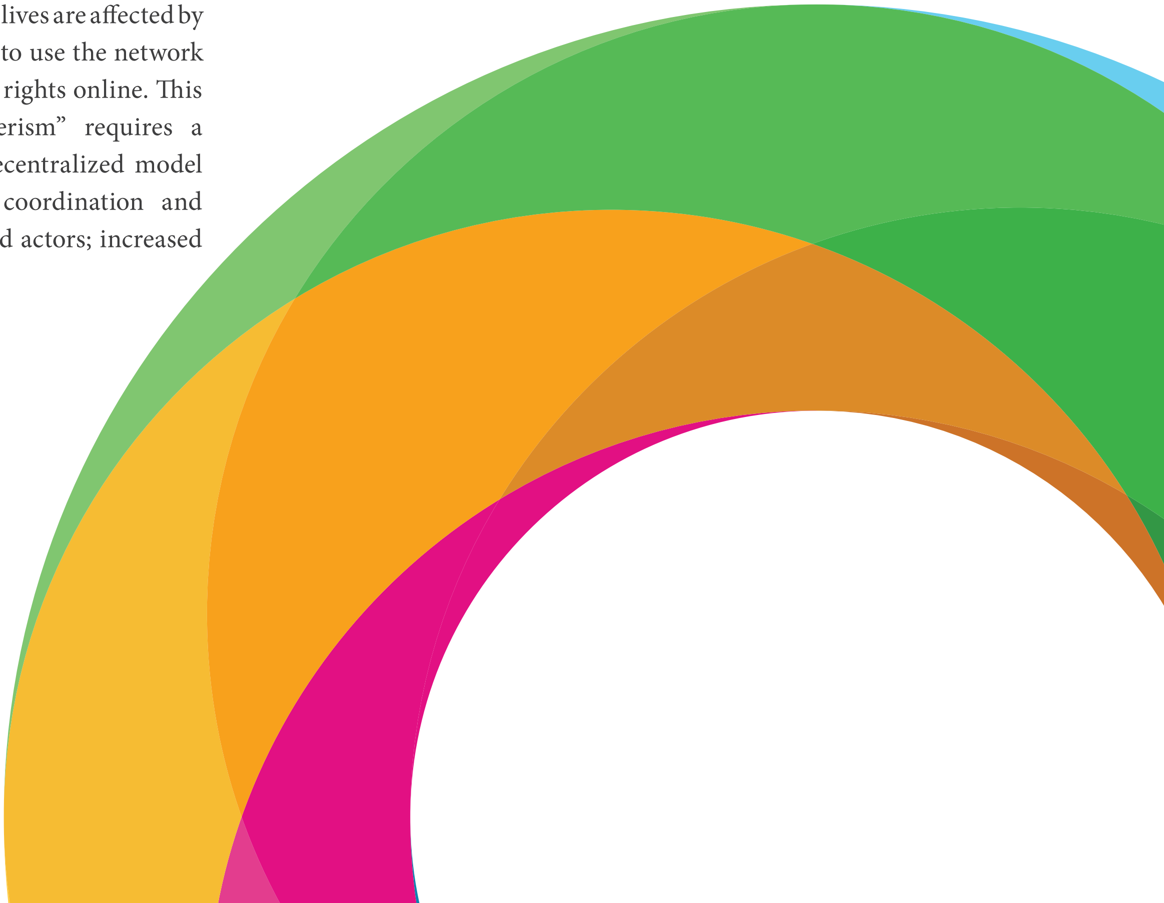
The Internet has indeed reached a crossroads. Choices need to be made — and making no choice is itself a choice. It is all about who should have what power to control the future of the Internet. The Internet has fundamentally altered the world, and as the next billion and the next after that join the 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 Global Commission on Internet Governance 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.



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