Internet Society

2017

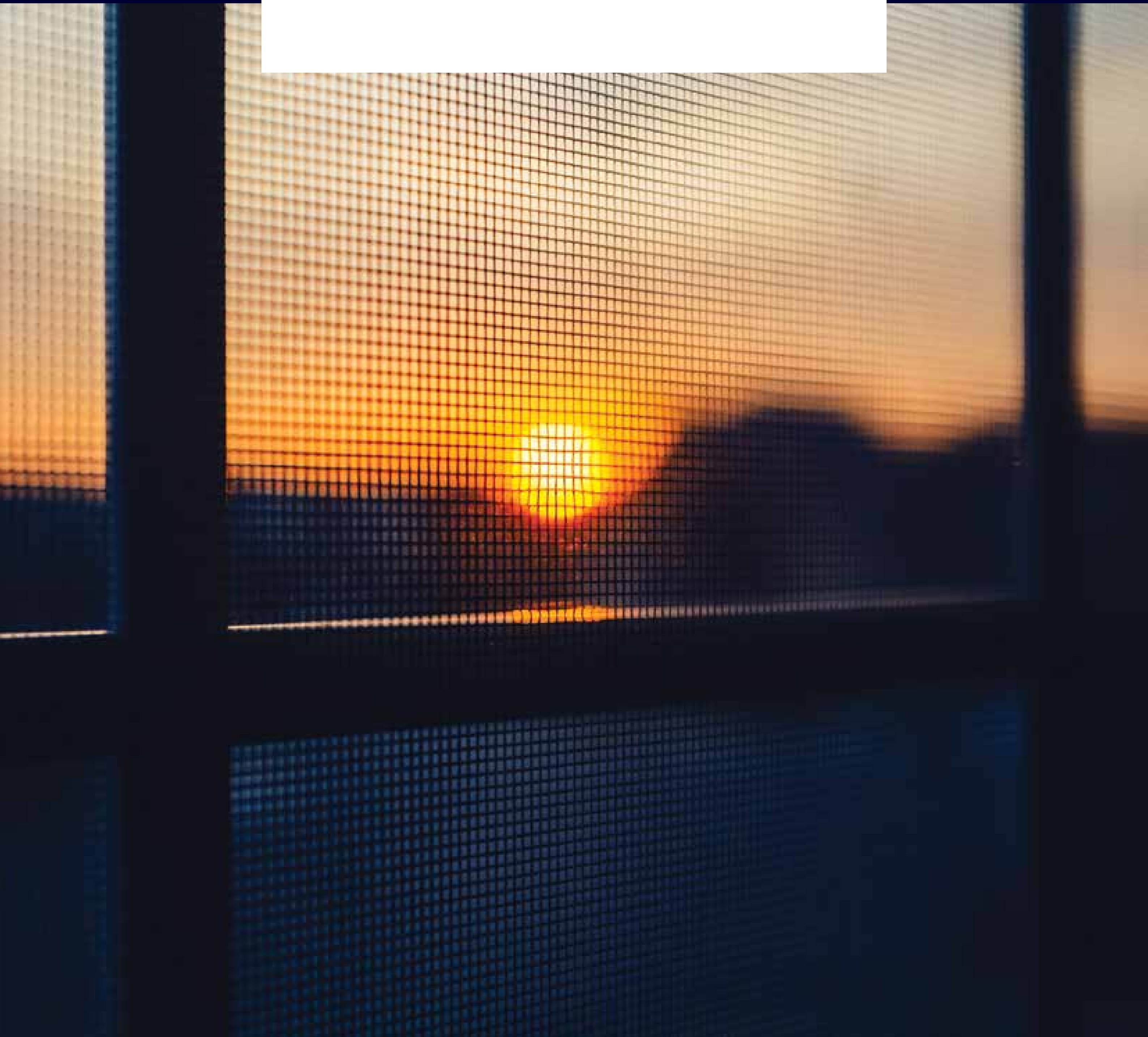
INTERNET SOCIETY GLOBAL INTERNET REPORT

Paths to Our Digital Future

Table of Contents

1

Foreword



Foreword by Kathy Brown, President and CEO, Internet Society

The Internet Society's history is inseparably tied to the history of the Internet itself. We were founded in 1992 by Internet pioneers Bob Kahn and Vint Cerf, along with numerous other visionary individuals and organisations. These early Internet luminaries believed that 'a society would emerge from the idea that is the Internet'. And they were right. The Internet has come a long way since its inception, and is now part of our social fabric — essential to how we connect, communicate, create and collaborate.

2017 marks a significant milestone for the Internet Society. This year we celebrate 25 years of advocacy for a global, open, secure Internet that benefits all people throughout the world.

It also presents an opportunity to take a look back at our roots and, most importantly, to look ahead to the future. This is an ideal moment in time to reflect on the Internet's meteoric rise and to imagine its future direction. As the Internet ecosystem becomes increasingly complex, so too do the challenges it faces. We know it will continue to evolve, but how?

The Internet Society's fourth annual Global Internet Report — Paths to Our Digital Future — explores this important question. This comprehensive report brings together insights from across our diverse global community to inspire all who engage with the Internet to think differently and to prepare for the opportunities and challenges on the horizon.

No one knows exactly how the Internet will evolve, but we do know it will require new thinking, new approaches and new tools for this rapidly changing world around us.

At the Internet Society we are committed to shaping the Internet's future for the next generation. Join us — **#thenext25**, **#shapetomorrow**.

2

Executive summary

Executive summary

The Internet has profoundly shaped our world and has changed our lives in both big and small ways. The technology change around us has happened both quickly and imperceptibly. The very first connections between computers nearly fifty years ago have been transformed into a wave of connectivity that covers the planet. New devices and innovations have given us more ways to harness the power of connectivity wherever we go and have given us functionality we could never have imagined.

We shouldn't underestimate the fundamental changes that faster, more affordable access to the Internet has already brought and will continue to bring to humanity. The question is whether we are ready for what's coming next.

Now is a big moment for the Internet. As we engaged with our community in the development of this report, it became clear that people are anxious about the future of the Internet. Some see a frightening future that awaits us in a technology-driven world. There are conflicting views around whether the Internet is a positive or a negative influence and while it becomes more and more central to our modern lives, we find that some are beginning to reject the globalised world view that it has fostered. On the other hand, communities just coming online see the Internet as "life" — as their connection to opportunity and freedom — and they want a chance to influence its future.

This report serves to remind us that humans are at the very heart of the Internet. It reminds us that every one of us has a stake. Recognising this responsibility, the report suggests that we need to begin to think differently to acclimatise to the changes we are seeing. Just as the Internet is a mirror to society, we must better understand that it will reflect both the good and the bad that exists in the world. Most importantly though, this report reasserts our belief that the Internet belongs to everyone and that, as its custodians today, we all have a duty to shape its future.

Our hope is that the insights and recommendations put forward in this report will play a role in helping us all to set the Internet on the path that best serves the needs of an evolving society in the years to come.

Report background

In 2016, the Internet Society launched a project to better understand the forces of change that will shape the Internet over the next five to seven years. We engaged with a broad community of Members, Internet Society Chapters, experts and partners. We conducted three global surveys and two regional surveys that generated more than 3,000 responses from 160 countries. We also interviewed more than 130 Internet experts and users, and hosted more than 10 roundtables.

Through these surveys and interviews, the community identified six key forces — or 'Drivers of Change' — that will have a profound impact on the future of the Internet in the years to come:

- The Internet & the Physical World
- Artificial Intelligence
- Cyber Threats
- The Internet Economy
- Networks, Standards & Interoperability
- The Role of Government

The Drivers encompass technological, economic, regulatory, security and network related challenges for the Internet of the future. In all cases, each force of change is inextricably tied to the other Drivers — for example, we fully expect to see an expansion of the role of government in Internet decision-making as a consequence of result of growing and ever more serious cyber threats. Or, we can see that standards and interoperability are crucial to the future of the Internet of Things. In the hyperconnected world of tomorrow, these Drivers of Change will be increasingly interwoven, presenting ever more complicated social, economic and policy challenges for society to grapple with.

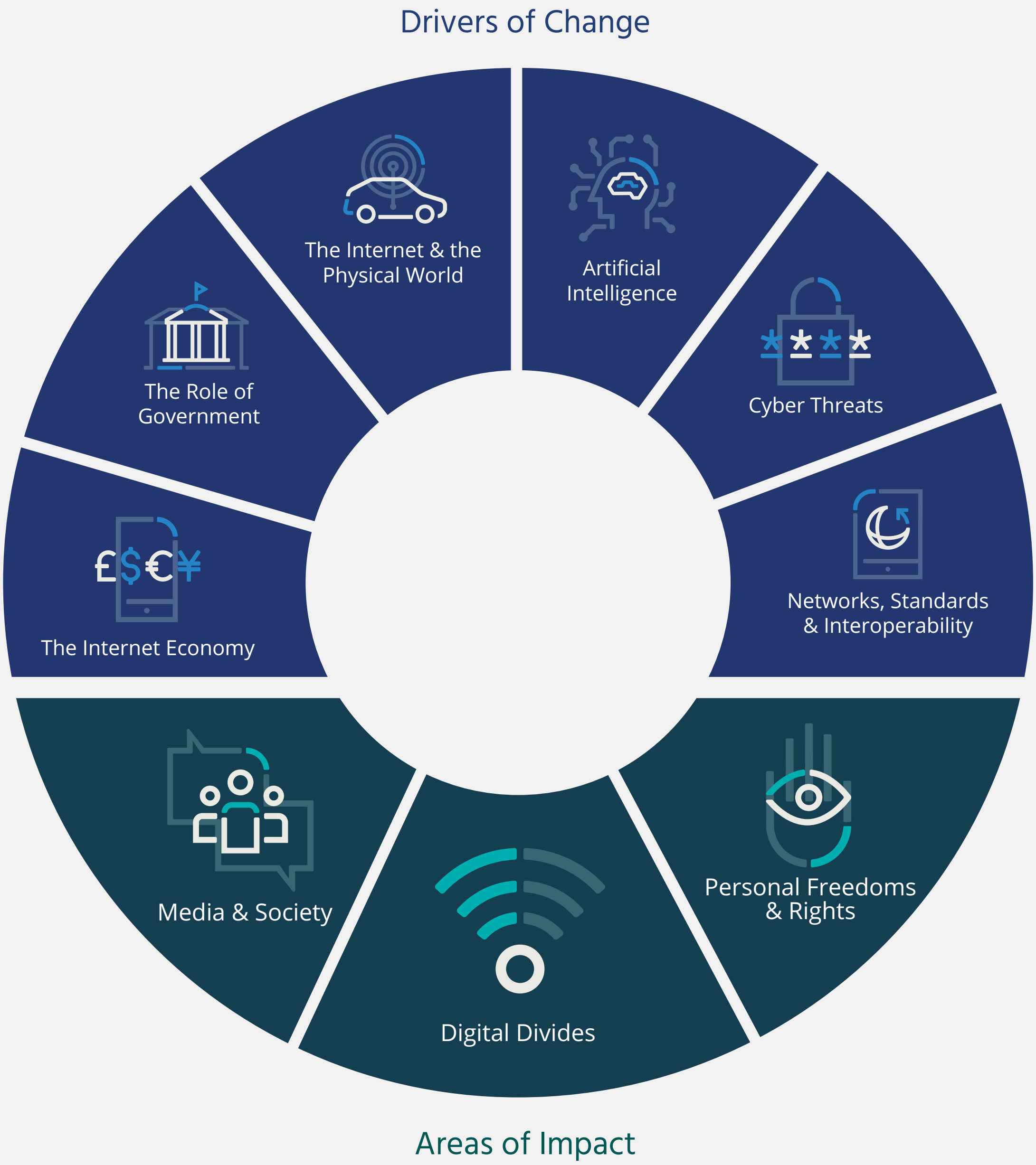
While these six Drivers of Change are interesting and important, what was clear from the outreach conducted was that the global Internet community is looking at these Drivers through the lens of three areas of impact. These are:

- Digital Divides
- Personal Freedoms & Rights
- Media & Society

These Areas of Impact are consistent with the Internet Society's mission to put the user at the centre of the equation when considering the future of the Internet. The ability for a user to connect, speak and share, as well as to innovate, choose the services and information they want to access, and trust the network, will all be impacted by the Drivers of Change.

For example, while the Internet of Things (IoT) will certainly influence the future Internet landscape, our community was focused on the implications of IoT for security or privacy (Personal Freedoms and Rights). And just as all sectors of the global economy will be transformed by the Internet, the question for us is whether this transformation will bring about *global* benefits or whether some parts of the world will fall further behind (Digital Divide).

Both the Drivers of Change and the Areas of Impact highlight the challenges and opportunities that users, communities and societies will face in the immediate future. And as the Drivers of Change and Areas of Impact were further discussed, and the breadth of the challenges and opportunities considered, some overarching themes were identified:



- There is a sense of both optimism and disillusionment about the future promise of the Internet.
- The rise of nationalism is challenging our basic notions of global interconnectedness and threatens to fragment the global Internet.
- Civil Society is seen as more important than ever, but support for it is seen to be declining.
- The Internet must remain user centric for it to be trusted and for its future potential to be realised.
- Addressing cyber threats should be *the* priority — it is critical for individual safety and for the future Internet economy.
- New thinking, new approaches and new models are needed across the board, from Internet policy to addressing digital divides, from security approaches to economic regulation.
- Multistakeholder approaches to Internet policy will become ever more relevant in a world in which the physical and the digital worlds converge and as the cross-border nature of Internet challenges becomes clear.
- Ethics will grow in importance as technical innovation accelerates and impacts people's lives.
- We are seeing what it means for the global Internet to reflect society; we should not be surprised that bad behaviours from the offline world are seeping into the online world.
- The core values and technical properties of the Internet remain as important as ever.

Conscious of the need for a way forward to address the challenges before us, we conclude the report with a set of recommendations derived from input from our community. These offer a basis on which policymakers, technologists, business persons and activists can act — as soon as possible — to ensure that the future Internet remains user centric, that it upholds and reasserts our freedoms and rights and that it continues to work for the benefit of all.

Drivers of Change

We can expect the world to change fundamentally over the next five to seven years with the convergence of the **Internet and Physical Worlds** and the deployment of the Internet of Things (IoT). When everything that can be connected is connected, whole economies and societies will be transformed. Services will become more efficient and data driven, providing new ways for us to interact with the world around us. However, increased security threats and device vulnerabilities, as well as incompatible standards and a lack of interoperable systems, could well undermine the technology's promise. Without appropriate safeguards and deliberate efforts to ensure transparency and user control, IoT could drive data collection and use in ways that further undermine privacy.

The advent of **Artificial Intelligence** (AI) promises new opportunities, ranging from new services and breakthroughs in science, to the augmentation of human intelligence and its convergence with the digital world. While there is significant hype about the possibilities that AI may bring, voices of concern about its unfettered development without appropriate human-centred safeguards are growing. In particular, ethical considerations must be prioritised in the design and deployment of AI technologies. We must ensure that humans remain in the "driver's seat" and that serendipity and choice are not undermined.

Perhaps the most pressing danger to the future of the Internet is the rising scope and breadth of **Cyber Threats.** As new technologies such as AI and IoT increase our dependence on the network, the severity of security challenges and vulnerabilities grows in parallel. At the same time, the continued success of the Internet as a driver for economic and social innovation is tied to how we respond to these threats. Insufficient attention to security will undermine trust in the Internet. Indeed, human safety is at stake. Stakeholders must do more to mitigate cyber threats — we may need to consider new accountability, incentive and liability models to encourage stakeholders to dramatically increase cybersecurity readiness and reduce vulnerabilities.

Yet, we cannot afford to let the 'securitisation' of the Internet, and our digital lives, run rampant: there is a very real threat that online freedoms and global connectivity will take a back seat to national security. Given the growing pressure from cyber threats and security challenges such as terrorism, the ease with which our open societies and our freedoms and rights could become subordinate to pervasive surveillance regimes facilitated by AI and IoT should not to be underestimated.

How we manage the deployment of IoT and AI, and how we address the growing cyber threat will determine whether we reap the benefits of what one community member called the next industrial and technological “Renaissance”. We are on the verge of a technological transformation that will disrupt economic structures and force businesses to think and act like technology companies as billions of devices and sensors connect to the network. The hyperconnected **Internet Economy** that results will see traditional industries morphing, emerging economies thriving and new market leaders from around the globe driving innovation and entrepreneurship. Yet, it is far from clear whether this technology-driven disruption will favour the existing Internet platforms or bring greater competition and entrepreneurship. Stakeholders will need to work together to ensure that they are appropriately equipped to adapt to the economic and social pressures the new Internet economy will bring.

This state of change will also shape the evolution of **Networks, Standards and Interoperability** and the architecture of the Internet. A proliferation of connected systems and mobile devices will result in ubiquitous connectivity requiring greater bandwidth and interoperability. The network edge will become more complex with large numbers and types of devices connecting to multiple new services, such as IoT; and, the nature of transit will change with the increasing use of CDNs, caching and other specialised services that flatten the network hierarchy. Taken together, the evolving edge and decline in transit may put pressure on the general-purpose Internet and its ability to support competition, and ongoing evolution and innovation. Additionally, developers are increasingly relying on proprietary standards which will be a barrier to innovation and interoperability. Open standards development will need to evolve to ensure standards are still relevant in a world of competing proprietary systems.

Finally, governance models and policies must evolve. As the Internet grows and expands into more areas of our economy and society, **Governments** will be faced with a host of new and complex issues that will challenge all aspects of their decision-making. Their responses to these challenges will impact not only freedoms and rights and the economy, but also the Internet itself. New technologies and game-changing business models will force governments to work differently — today’s structures and policies will be quickly outdated. Internationally, cyber security issues will drive global governance discussions for the foreseeable future, with governments pressured to make decisions that could undermine the open and distributed global governance of the Internet. Populist trends around the world will undermine decades of interconnected policy goals in ways that could fragment the core architecture of the Internet and undermine its global promise. Despite broad recognition of the need for multistakeholder approaches to Internet policy, the awkward dance between multistakeholder and multilateral approaches to Internet policy at the international level will continue.

Areas of Impact

While the future of the Internet depends on how technology, policy and economic factors play out, it was clear that our community was focused on the implications of these changes on some key vectors — Personal Freedoms and Rights, Media and Society, and the Digital Divide — the Areas of Impact.

Data shows that, while we still have a long way to go, the **Digital Divides** as we have historically defined it — those who have access to the Internet versus those who do not — is closing. Yet, the threat of new divides will emerge in the future, driven by developments in technologies and networks, as well as by the lack of economic opportunity and cyber readiness. As the Internet continues to transform every sector of the global economy, the digital divides of the future won't just be about access to the Internet, but also about the gap between the economic opportunities available to some and not to others. These new divides will not only deepen disparities between countries — in particular, between developing and developed nations — but also within countries.

Perhaps most worrying is the increasing likelihood of a security and trust divide: cyber threats will continue to multiply and users who lack the skills, knowledge and resources to protect themselves and their data will be far more likely to become victims of cybercrime. Thus, we will see a divide emerge between the security "haves" and the "have nots". Addressing this digital security divide will be critical to realising the full potential of the future Internet.

The future of the Internet is inextricably tied to people's ability to trust it as a means to improve society, empower individuals and enable the enjoyment of **Personal Freedoms and Rights**. Younger users and those in developing countries are particularly optimistic about the future of the Internet and the ability to use the technology to better their lives and create their futures. Yet, the Internet also brings challenges to human rights like privacy and free expression. Technologies like Artificial Intelligence and the Internet of Things will enable the generation and collection of enormous amounts of information about individuals that can be analysed in ways that are deeply personal, raising the potential for a "surveillance society" to emerge. At the same time, these technologies and applications also provide the potential to enhance these personal rights and freedoms, but only if ethical considerations steer technology development and guide their use.

We worry that as the scope and severity of cyber threats continues to grow, and as global Internet platforms are used to deliberately spread disinformation, users will lose trust in the Internet. Governments are under increasing political, economic and social pressure to respond to cyber threats, terrorism and violent behaviour online. Measures that may be intended to secure cyberspace will increasingly undermine personal rights and freedoms. Without a change of course, personal freedoms and rights online may well be nearing a point of irreversible decline.

The relentless march towards ever greater levels of connectivity will continue to bring new shifts in **Media and Society**. Emerging technologies and the growing interconnectedness of our economies will continue to shape social practices, how communities are formed, how opinions are shared. As the Internet evolves further, we can expect it to bring new pressures that will impact our interaction across the converging online and offline worlds in new ways.

The changing media ecosystem will continue to evolve, bringing new voices, but also less trust. While democratising access to information, the whirlpool of information and misinformation that exists online is raising real concerns about the long-term effects of new trends such as fake news. Unfettered extremism online and uncivil behaviour that breaks social conventions will erode social cohesion, trust in the Internet and even political stability.

Beyond this, as AI and automation change the labour market and displace some jobs while creating new ones, an economy that is more and more data-driven will create challenges for accountability and transparency. The lines between public and private sectors will blur and considerable anxiety may be created in the short term as people worry about the future of work and whether they have the skills to succeed in the new economy. It will be critical for society to plan for these disruptions in order to protect against the negative consequences they bring for people and communities.

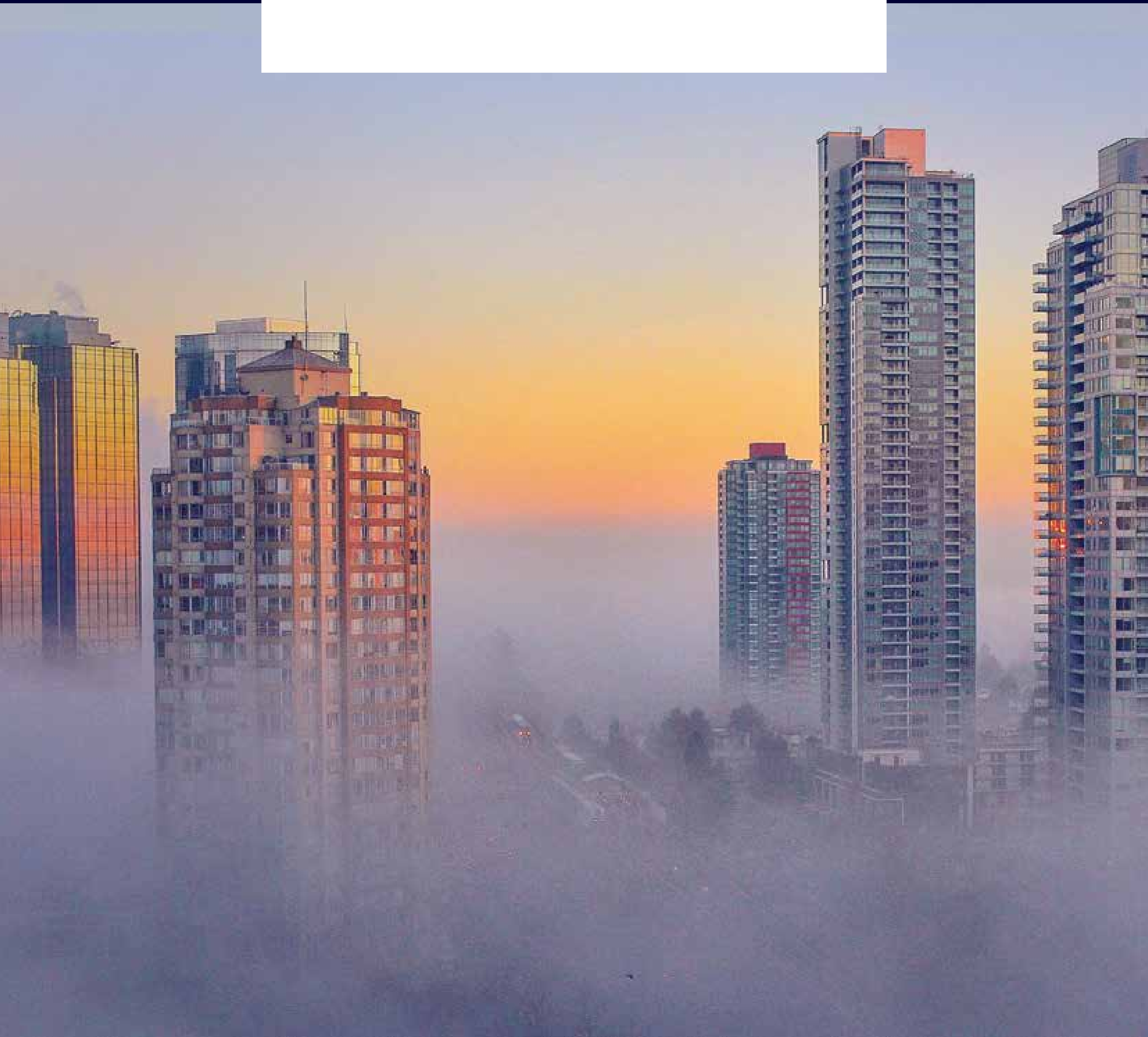
Recommendations

In the Drivers of Change and Areas of Impact, the community identified a range of future challenges and opportunities. To help decision-makers address those challenges and benefit from the opportunities, the Internet Society asked its community to also suggest ways forward, solutions and other approaches for governments, businesses, civil society and other stakeholders to consider.

Some of the recommendations are targeted at specific stakeholders; others are designed to provide general food for thought. In all cases, the recommendations are focused on things that can be done now to rebuild trust in the Internet and to ensure that the users, individuals and citizens of the future can fully benefit from the socioeconomic opportunity the Internet can bring.

3

Introduction



Introduction

No one can predict the Internet's future, but it is too important to ignore. Most believe the Internet will continue to shape our societies, cultures and economies, and define the world for generations to come. But there are no assurances of what lies ahead for the Internet. The choices we make today will impact the Internet we are creating for tomorrow.

From its earliest beginnings, the Internet evolved from a set of fundamental principles based on openness, inclusivity, collaboration, and transparency. While its original premise was the voluntary exchange of data across a network of networks, its social, technological, economic and political impact has been profound.

The future Internet promises social development, economic prosperity, and new technologies that can amplify the best of humanity. But it also brings about daunting challenges and questions.

> “
>
> It is difficult to predict, especially the future.
>
> Niels Bohr

The Internet Society launched an initiative in 2016 to identify the uncertainties and factors that will shape the future of the Internet. Distinct from other Internet industry research initiatives, this has been a community-based endeavor to draw from the expertise and diverse experiences of stakeholders across our global community. Through a series of interviews, surveys and consultations with key stakeholders over an 18-month period, a picture of the future has emerged. This picture suggests that while technology will permeate virtually all aspects of society in ways we have yet to fully imagine, the foundational values of the Internet will remain as important in 5-7 years as they did 25 years ago.

Our goal for this report was to explore the hopes and fears for the future of the Internet guided by a central question: *How do we ensure the continued development of an Internet at the service of all people?* What became evident throughout this work is that, while the Internet Society community is rooted in a deep commitment to the core technical properties of the Internet, there is a clear need to focus on both the technical development of the Internet as well as the opportunities for human empowerment that it enables.

The observations we collected are fascinating, reflecting the vast diversity of our global community and the Internet. Many young people described the Internet as “life”. In emerging economies, we heard great optimism about the hopeful prospects that the Internet holds for them. Others expressed disillusionment and questioned how cyber threats, the Internet of Things and government interventions might reshape the Internet and society.

While there were differing views on some topics, we found many common threads. Six dominant forces emerged as the greatest Drivers of Change and concern for our global community. Looking at the effect of these drivers on individuals, we explored them through the lens of three important Areas of Impact: the Digital Divide; Personal Freedoms and Rights; and Media and Society.

The totality of such dynamic processes is impossible to capture in one report, but by describing the interlinkages among these different Drivers, and the relationship to the three Areas of Impact, we aim to provide the reader with valuable insights to the scope of the challenge before us.

As we envision what may lie ahead, the report offers an eye-opening collection of “What if” vignettes. These fictional stories provide a peek into how the Internet might evolve. Finally, as an outcome of this extensive research, the Global Internet Report provides an actionable set of recommendations to encourage our community, stakeholders, activists, and influencers toward positive actions.

We cannot take the Internet for granted. The path to our digital future rests in our hands. We can start today by taking actions that will preserve the underlying values of the Internet and keep it on course to remain open, globally connected and secure.

We hope that this glimpse into the future will inspire readers to get engaged and to join us as we work to ensure a future Internet that reaches everyone, everywhere and expands opportunity for all.

4

How we see the Internet

How we see the Internet

When we think about the Internet, many of us think about something beyond the technology of the Internet itself. By definition, the Internet is a technical system: a communications infrastructure that enables networks around the globe to interconnect. However, over the past two decades, the Internet has become far more than a technology. With more than 3.5 billion people online today, the Internet is now an integral part of the social and economic fabric of many communities around the world.

Based on the views expressed in the interviews that inform this report, we use the term 'Internet' to refer not only to the technical infrastructure, but also to the entire social and economic ecosystem to which it has given rise.

> **The Internet Society capitalises the term "Internet" to differentiate the global Internet from generic "internets", which can refer to any interconnected group of computer networks.**[1]

Fundamental properties of the Internet

In the history of humankind, few technologies have resulted in such widespread social and economic change in a relatively short period of time. Growing nearly 900 per cent from 400 million in 2000 to 3.5 billion users today, the Internet has had an unprecedented impact on the economy and societies around the globe.

Conversely, the impact of the Internet on society has also transformed the Internet itself. It is no longer just the home of email, static webpages and discussion boards. Today's Internet is so much more. It is a dynamic space for collaboration, commerce and expression. Video currently accounts for more than two-thirds of all Internet traffic in the world, and people accessing the Internet via a mobile device now outnumber those connecting from a computer. The Internet has changed political systems, revolutionised business, and reshaped communities worldwide.

In spite of all this dynamism, certain properties of the Internet persist. These properties, which we call *invariants*, have been the foundation for the Internet since its earliest days. At the same time, it is because of these invariants that the Internet has become such a dynamic resource. These technical properties are at the heart of the Internet's success — they provide users with the ability to fully benefit from the Internet.

[1] https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

Internet Invariants

Global reach, integrity
The Internet's routing, naming and addressing service ensures it is truly global. An Internet user can reach websites, email addresses, smart phones or any other Internet connected devices and is able to trust that the information received is the information requested.

General purpose
The Internet has no inherent limitations on the applications and services it supports. The Internet supports more than the World Wide Web and email.

Supports innovation without requiring permission
As an entrepreneur or creator, you don't need to ask permission to create a new service on the Internet. This "permissionless innovation" is crucial to the Internet's success; it removes the barriers to entry. From the World Wide Web to social networking, from BitTorrent to Bitcoins, many of the applications that billions of Internet users use every day were only possible because of this permissionless innovation.

Accessible
There are no limitations on who can access the Internet; all that is required is a connection. Anyone can use their connection to create and share content, but also to attach entirely new networks such as small, local community networks.

Based on interoperability and mutual agreement

The Internet is a network of networks. It works because those networks can communicate with each other, based on open standards for the technologies that support it and through the agreements made between network operators. Jari Arkko, former chair of the IETF, perhaps said it best: "I cannot think of a better example where interoperability is more important than the Internet of Things. Without interoperability, lights won't work with the switches, sensors can't be read by your smartphone, and devices cannot use the networks around them".[2]

Collaboration

The various stakeholders who support the operations of the Internet collaborate to ensure the Internet continues to work, grow and develop. This spirit of collaboration exists even among competitors in the private sector and between stakeholder groups that might not otherwise collaborate (for example, between the technical community and civil society). Collaboration when needed, competition when possible.

Technology, reusable building blocks

The Internet is comprised of numerous technologies that together create the Internet as we know it today. However, each individual technology, or building block, may be used for purposes for which it was not initially developed. There should be no restrictions on the functions of the technologies that comprise the Internet being used for future innovations.

No permanent favourites

The Internet has no favourites. In the 1990s, Netscape and Mosaic were among the most popular browsers on the Internet. Before Facebook and Twitter, MySpace was the dominant social network. Today, more people access the Internet with a mobile device instead of a desktop computer. New technologies and applications often replace older ones, and this is part of the natural evolution of the Internet.

[2] Blog by Jari Arkko, An Interoperable Internet of Things: https://www.ietf.org/blog/2016/01/an-interoperable-internet-of-things

The principles that guide the Internet Society's work

The Internet Society believes that the Internet empowers users with certain *abilities*. These abilities underpin the social value that the Internet provides to people. As we look to the future, these abilities must remain at the heart of the Internet experience for everyone, everywhere.

The ability to Connect

The Internet was designed to ensure anywhere to anywhere connectivity. All Internet users, regardless of where they live, should have the ability to connect to any other point on the Internet, without technical or other impediments. This ability to connect people is essential to the Internet's value as a platform for innovation, creativity and economic opportunity.

The ability to Speak

The Internet's value as a medium for self-expression is dependent on the ability of its users to speak freely. Private, secure and — when appropriate — anonymous communications ensure that Internet users can express themselves in a safe and secure manner. All Internet users should have the means to communicate and collaborate without restriction.

The ability to Innovate

The growth of the Internet is the direct result of the open model of Internet connectivity and standards development. Any individual or organisation should have the ability to develop and distribute new applications and services, free of governmental or private sector restrictions for anyone to use.

The ability to Share

The Internet enables sharing, learning and collaboration. The ability to share has given rise to the open development of the key components of the Internet, such as the Domain Name System (DNS) and the World Wide Web. Fundamental to this ability is the concept of fair use, and the freedom to develop and use open source software.

The ability to Choose

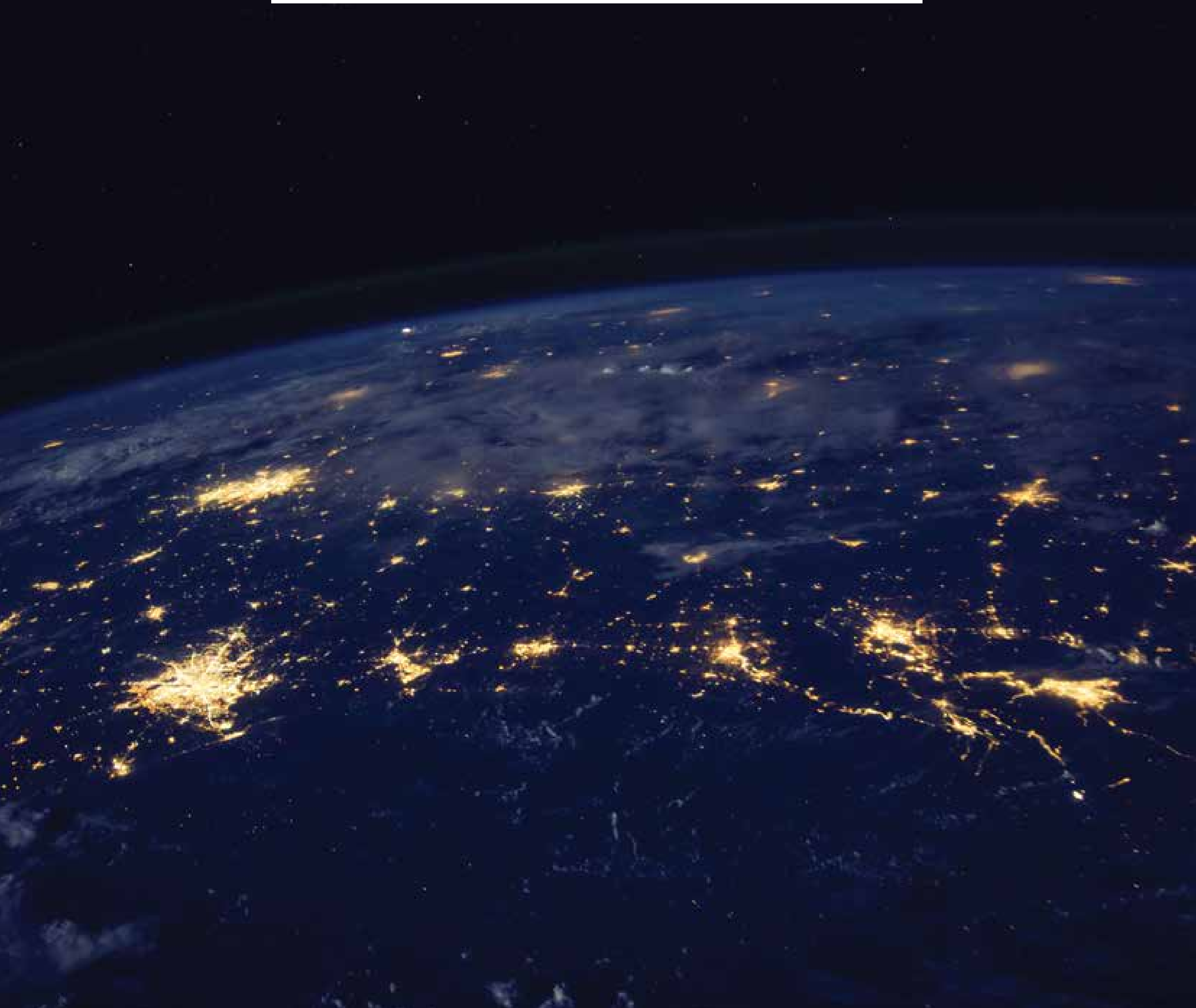
User choice and competitive communications markets result in the availability of better, cheaper, and more innovative Internet-related services. An Internet access environment characterised by choice and transparency allows users to remain in control of their Internet experience.

The ability to Trust

Everyone's ability to connect, speak, innovate, share and choose hinges on trust. The security, reliability and stability of the network, applications and services is critical to building online trust.

5

Drivers of Change & Areas of Impact



Drivers of Change & Areas of Impact

Drivers of Change

The Drivers of Change encompass technological, economic, regulatory, security and network related challenges for the future Internet. In all cases, the implications of one Driver are inextricably tied to another — for example, we fully expect the Role of Governments in the Internet to grow in large part due to the rise of Cyber Threats.

Each of the Drivers of Change is presented in the following format:

- Introduction of the Driver and key takeaways
- Vignettes, or stories that illustrate ways in which each Driver could shape the Internet in the future
- Two or three issues areas that demonstrate the impact of the Drivers on each other and the Areas of Impact

The Drivers of Change are:

- The Internet Economy
- The Role of Government
- The Internet & the Physical World
- Artificial Intelligence
- Cyber Threats
- Networks, Standards & Interoperability

Areas of Impact

Throughout the project, our community has reaffirmed the importance of three issue areas that are crucial for the future Internet: Digital Divides; Personal Freedoms and Rights; and Media, Culture and Society. These Areas of Impact reflect the Internet Society's fundamental belief that the interests of the user and society must remain at the forefront of any discussion on the future of the Internet. Each Driver of Change has implications for one or more of these Areas of Impact.

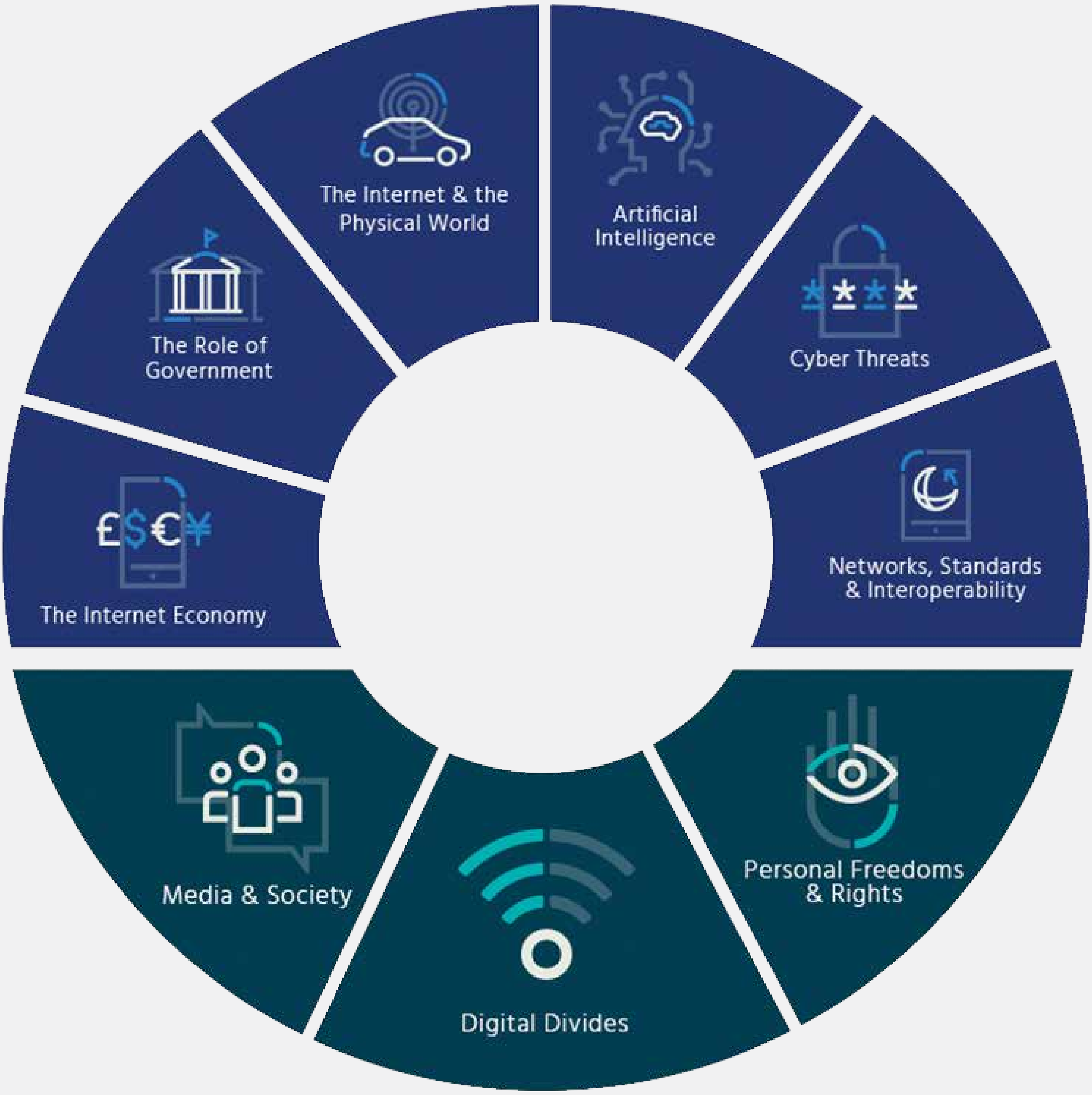
Each of the Areas of Impact is presented in the following format:

- Introduction of the Area of Impact and key takeaways
- Vignettes that illustrate the ways in which the Area of Impact could evolve in the future
- A visual overview of how the Drivers of Change will affect the Area of Impact in question, followed by a more detailed overview of the related challenges and opportunities

The Areas of Impact are:

- Media & Society
- Digital Divides
- Personal Freedoms & Rights

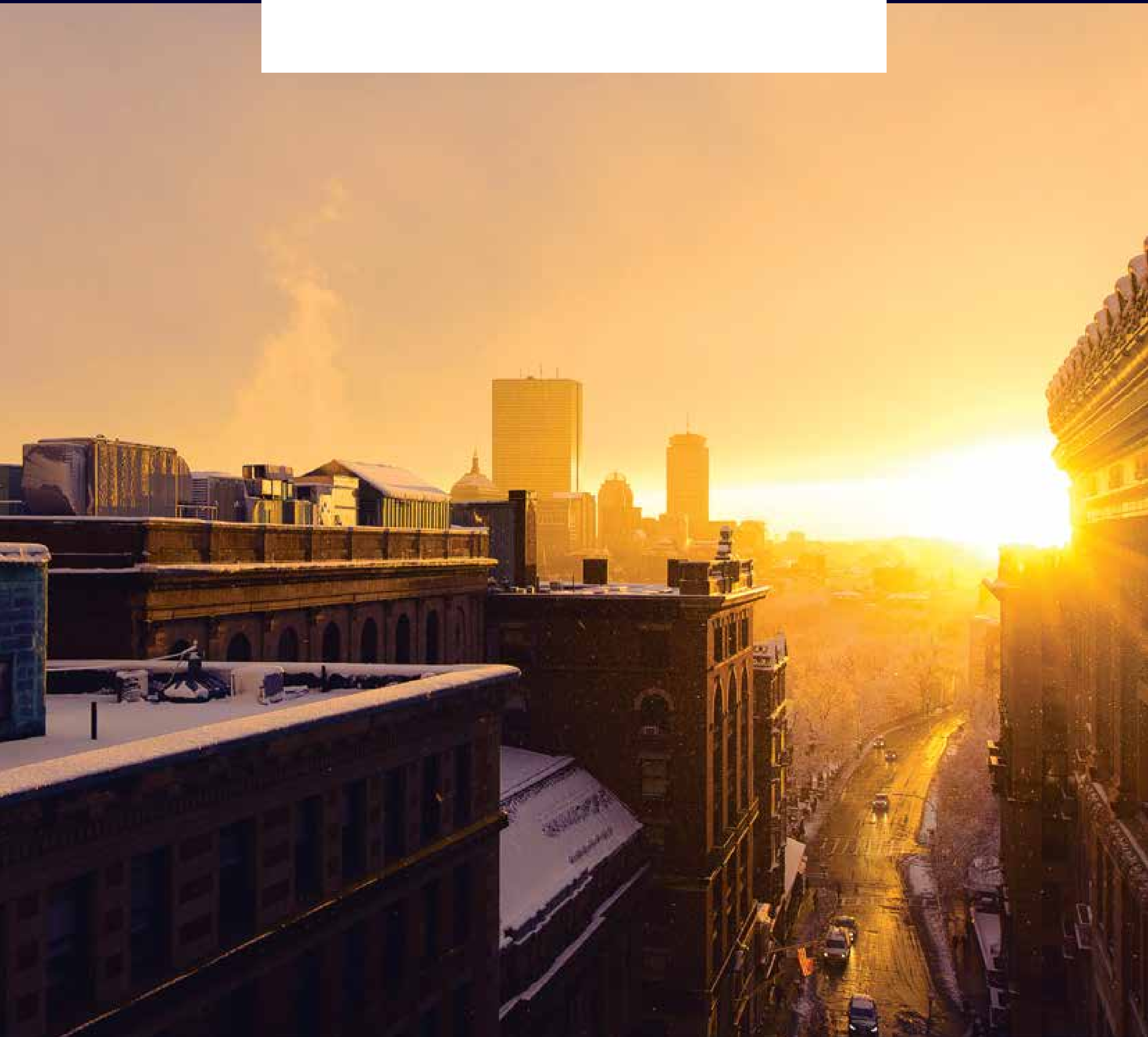
Drivers of Change



Areas of Impact

6

Drivers of Change



The Internet Economy

In a hyperconnected world, no sector of the economy will be untouched by technology and only those who adapt quickly to technological change will be successful.

Overview

The Internet economy will evolve substantially over the next ten years, fueled by innovations in technology and business models. Advances such as the Internet of Things (IoT), Artificial Intelligence (AI), and blockchain could bring about an industrial and technological "renaissance". Our community believes that the Internet will promote drastic shifts across all sectors of the future Internet economy. In a hyperconnected economy, no sector of the economy will be untouched by technology — hospitals, transportation companies, manufacturing firms — and only those who adapt quickly to technological change will be successful.

This rapid change will disrupt businesses and increase pressure on societies, particularly on jobs and economic opportunity. Business models and the nature of work will be profoundly changed. It is far from clear whether this technology-driven disruption will favour existing Internet platforms or bring greater competition and entrepreneurship. Either way, governments and society at large will need to quickly adapt to the new economy and its policy challenges.

We are on the verge of a technological paradigm shift as the digital and physical worlds converge. This technology "renaissance" will disrupt existing economic structures and business models in ways that society is only beginning to understand.

All parts of society — from local communities to education systems, healthcare and public services — will have to adapt to the pace of change.

Governments, and particularly policy-makers, will be ill equipped to respond to the economic and social pressures of IoT and AI.

Market consolidation by Internet service and access providers could spur the growth of so-called "walled gardens" — closed platforms with proprietary ecosystems — leading to a loss of choice, constraints on innovation and Internet fragmentation.

Those economies and new market leaders who successfully anticipate this paradigm shift will drive innovation and entrepreneurship.

The Impact of New Technologies on Industry and the Economy

The Internet economy will increase efficiencies, productivity and create new opportunities not yet imagined. The pace of technological change will dramatically accelerate as IoT, AI, and blockchain technologies are fully deployed. They will reshape economies in ways stakeholders, and particularly governments, may be ill-equipped to keep up with. And as technology drives automation, traditional jobs and the local economies that rely on them will be at risk. The future Internet economy will depend on new approaches to skills and education.

> I think the government knows how important IoT is for the entire economy in the coming years. Therefore, their response will be based on investing and deploying IoT and artificial intelligence, especially in building smart cities and industry.
>
> Internet Society Member, Middle East

New technologies and services, including currencies and payment models, will continue to challenge existing institutions and industries: many companies will be pushed into adopting new technologies just to stay competitive with new entrants. We will also see more mergers and acquisitions as bricks and mortar companies seek to integrate technology companies, and vice versa. These forces could radically reshape industries and business practices, impacting every economic sector. Governments may need to increase spending on training programs to help workers impacted by technological displacement.[1]

> Many Internet trends are expanding into the social environment, for example Airbnb but also smaller firms that, for example, cook food at home for customers or that invite customers home. Such trends will clash with established business models, but are needed to give people more flexibility and to allow new models to evolve.
>
> Private Sector, Europe

[1] https://www.technologyreview.com/s/603465/the-relentless-pace-of-automation/

> Every industry leader in every economic sector is at risk of being disrupted. The economy changes far faster than the rules governing it. The system we have in place to regulate business is stuck on twentieth-century notions of how the economy works — some of which no longer make sense.
>
> Private Sector, Europe

Traditional manufacturing sectors that were once relatively insulated must evolve to succeed in an increasingly connected Internet economy. As devices and appliances are built to be network ready, the line between manufacturer and tech company will blur. Companies will need to adopt a technology mindset as they move from replacing parts to updating software. The growth of IoT will effectively make *all* companies technology companies. This shift to greater dependency on technology will be accompanied by new security concerns. As one survey respondent in North America noted, "losing control of your data is catastrophic today. Tomorrow, it could mean the death of your business".

> Business is trying to protect against disruptions to their business models – for example, in the tussle between Google's automated cars and the automobile industry. For one, it's just another application of sensor technology, for the other, it's a change in mindset.
>
> Academia, Asia-Pacific

Digital currencies could also transform the global financial system. For example, digital currencies can support financial inclusion because they allow people to transfer funds without an intermediary; they also provide alternatives for those in countries experiencing currency volatility. The future of digital currencies will be determined by the next generation's willingness to embrace the technology, something our community remains uncertain of.

Whole societies are ill-prepared for the rapid pace of technological change. This risk may be more acutely felt where technology drastically outpaces the ability of some countries to keep up. In terms of digital readiness, the current gap between the top seven countries and those that follow is already wide. Understanding and managing the implications of new technologies, and the economic and societal forces that they will unleash, will be critical to economic development and competitiveness.

> Governments may face a dilemma due to the fact that AI and IoT will reduce employment opportunities in certain industries. On the other hand, they will have no choice but to move with the world trends… I can imagine having robots deployed underground to mine our copper and manage underground infrastructure.
>
> Internet Society member, Africa

Related to: Artificial Intelligence; The Internet & the Physical World

Market Consolidation, Walled Gardens and Policy Responses

In this future technological "renaissance", will today's most widely-used online services and platforms deepen their market position, or face competition and possible displacement by new players? Could these Internet companies face new competition from traditional industries as they go online in a world of IoT? Our community, particularly among those from the private sector, is generally optimistic about a more competitive environment. However, if the Internet platforms of today consolidate their power — becoming dominant across infrastructure, services and applications — user choice and control over their online experience, as well as the availability and diversity of information and content, could be constrained.

> "
>
> Scalability is such an important factor in the Internet economy. When search companies reach such a level of scalability, it is difficult for others to compete with them. This issue will be a global issue.
>
> Government, Asia-Pacific

Without thriving competition, closed platforms and proprietary ecosystems, or "walled gardens", may proliferate. Customers may find it difficult to move from one provider or platform to another. This will result in the loss of choice and constraints on innovation and lead to Internet fragmentation.

> "
>
> There is a trend towards an ecosystem of users and developers, in which you can have the big winners or something similar to walled gardens. But there will always be some disruption that fragments this garden and creates a new paradigm.
>
> Private Sector, Latin America & Caribbean

"Walled gardens" could also arise as a reaction to political concerns such as economic isolationism and national security, hindering the development of the global economy. Among our community respondents from Africa and Asia reported a significant trend toward greater use of the global, public internet whereas respondents from Europe and North America reported significant trend toward greater use of closed, access-limited, or private IP networks.

How governments should respond, and whether their existing policy tools are adequate, will also be called into question. One survey respondent from the Middle East suggested that, " ...as governments begin to identify the potential of the Internet, there will be increased regulation for social and economic reasons". This said, the economy will change far faster than the rules governing it. As one private sector representative from Europe noted, "*The system we have in place to regulate business is stuck in the 20th century notion of how the economy works*". Legacy policy approaches will become increasingly counterproductive in the hyperconnected world of tomorrow. As technologies such as AI, IoT and blockchain roll out, there will be considerable growing pains as policy frameworks struggle to keep up.

> "
>
> Other trends concern the nature of governments to regulate that which they cannot understand. There is increasing pressure for governments who see free speech and permissionless innovation as a threat to crack down on political and economic dissidents alike.
>
> Private Sector, North America

Related to: The Role of Government; The Internet & the Physical World; Networks, Standards & Interoperability

The Future of Innovation and Entrepreneurship

A small number of major companies may further concentrate their power by absorbing potential threats or new opportunities. The reach and resources of Internet platforms mean that startups will be acquired in their infancy, before they can disrupt the bigger players. Will the idea of permissionless innovation and the notion that anyone can start the new "Google" still be realistic?

> "
>
> The question is if smaller entrepreneurs are going to be able to "compete" or get caught up in an uncertain environment of investment and competition from big conglomerates.
>
> Roundtable with Chapter Members in Africa

This said, innovation and new services on the Internet often develop and move faster than anyone can predict. Many big players and favourites of the past are now mere footnotes in the history of the Internet. Economic growth and business opportunity will increasingly depend on a dynamic and innovative Internet, which, in turn, will depend on open interoperable standards and permissionless innovation. This demand for continuous innovation by industry, users and even government may mean that even today's large Internet platforms will face fierce competition from emerging players, including those outside the traditional ICT sector.

> “
>
> We can no longer credibly argue that someone can create something new, start a new service in a lab and individually change the future. This isn’t necessarily bad, but it does have implications for policy, technology, industry. This really just reflects a maturation of an industry. We are moving/have moved from individual entrepreneurs to partnerships and alliances that drive innovation.
>
> Government, North America

A new generation of entrepreneurs coming online from emerging countries has the opportunity to use technology to solve local problems, reach global markets and drive innovation. As more people benefit from coming online in the next five to ten years, the opportunities and funding for entrepreneurs and startups will grow locally and globally. Startups will be able to scale more quickly, accelerating past the traditional path of company growth. And as Internet growth shifts from the historically strong digital economies in North America and Europe to emerging markets in Asia, Latin America and Africa, new innovation leaders and technology hubs will emerge. These new entrepreneurs should play a pivotal role in shaping the future of the Internet economy.

> **European respondents believe the greatest sources of Internet innovation and new Internet companies in the future will be today’s highly-developed economic regions. This is in contrast to respondents in Africa and Asia who believe that future innovation would come more from emerging or developing economic regions.[2]**

Related to: Digital Divides; Networks, Standards & Interoperability

[2] Future of the Internet Survey 2 - Question 4: “Which areas of the world are the greatest sources of Internet innovation and new Internet companies”?

Artificial Intelligence

Advances in Artificial Intelligence and Machine Learning will transform the world with such speed that society will struggle to address crucial ethical considerations and economic consequences.

Overview

Together, Artificial Intelligence[1] (AI) and the Internet of Things (IoT) will transform both the Internet and the global economy. Within the next five years, we can expect AI and machine learning to become imbedded in all forms of technology that incorporate data exchange and analysis. The opportunities this creates are immense, ranging from new services and breakthroughs in science, to the augmentation of human intelligence and its convergence with the digital world.

There are considerable uncertainties about AI, including the delegation of decision-making to machines, lack of transparency and whether technological change will outpace the development of governance and policy norms. Automation may profoundly change industry, affecting employment and the delivery of public services. Governments and societies need to prepare now for its effects.

Economies and societies must prepare for the disruption that AI (along with IoT) will bring.

Ethical considerations must be prioritised in the design and deployment of AI.

AI and automation will promise new socioeconomic opportunities, but the impacts and trade-offs for individuals and societies are unclear.

As AI changes how we make decisions, we must ensure that humans remain in the "driver's seat".

There is a high risk that the benefits of AI will be unevenly distributed within and across societies — exacerbating current and future digital divides.

[1] Artificial intelligence traditionally refers to an artificial creation of human-like intelligence that can learn, reason, plan, perceive, or process natural language.

Governance and ethics in a world of AI

AI raises extensive ethical concerns. Technologists themselves say the technology needs to align with human values, and that ethical dimensions must be prioritised at every stage of the design, development and deployment of AI systems.[2] The speed at which AI and related technologies are being developed and deployed will require significant investment and effort in the short term to avoid unintended consequences for society and humanity. We will need focused research and effective governance structures to make sure AI technologies create opportunities and not harm.

> “
>
> Algorithms are still being developed by people, at this point; we have a bit of control of what we are doing. However, if we concede all this to intermediaries and their algorithms, in five years’ time, they may not be developed by people. Are the intermediaries that we deal with going to be artificial intelligence?
>
> Academic, Europe

> “
>
> It starts with the value of the human. Once we start giving power to machines, will that be tied to the metaphysical commitment to the human at the center of governance? We don’t know what the consequences are.
>
> Civil Society, North America

AI also raises serious considerations related to privacy, transparency, safety, the nature of work and jobs, and the overall economy. For example, technologies such as facial recognition based on AI can improve user experience over a social media platform. But the same technologies can be used to improve surveillance and compromise anonymity. Or, if AI becomes a permanent feature in social media networks and online platforms, where algorithms are used to curate the online experience, questions about free choice and bias will intensify. Concerns about the transparency and accountability of data collection and decision-making will accelerate calls for ethical principles to guide AI design and deployment.

[2] https://futureoflife.org/ai-open-letter

> “
>
> A society completely based on data collection on the business side… fuels a surveillance society without proper democratic checks and balances. Humans lose some self-determination through automated choices by connected machines.
>
> Human Rights Expert, Europe

> **Our community, across all stakeholder groups and regions, believes that automation generated through data analytics technology will have greater influence on human behaviour and decision-making.**[3]

How will governments address the larger economic and social impact of AI, and will they have the skills and resources to do so? Within governments, AI could bring about a fundamental reshaping of decision-making as policy development is increasingly data driven. By extension, there is a risk that AI could become an unaccountable and non-transparent decision-making tool for future policy choices.

> “
>
> The development of IoT and AI will provide scientific references for government decision-making and help them to respond quickly to public needs.
>
> Technologist, Asia-Pacific

Many foresee a fierce, competitive battle to dominate the commercial AI space in coming years. While this will likely drive innovation and possibly disrupt current market structures, there are also concerns about competition. Forecasters believe that today’s leading technology firms will control the market for AI platforms for the foreseeable future.[4]

Related to: The Role of Government; The Internet & the Physical World; Personal Freedoms and Rights

[3] Future of the Internet Survey 2 - Question 22: “To what extent does the use, insights, and automation generated through data analytics technology influence human behavior and decision-making”?

[4] https://www.nytimes.com/2016/03/26/technology/the-race-is-on-to-control-artificial-intelligence-and-techs-future.html

Impact of AI on the Internet economy

While some argue that projections about AI are simply marketing hype, there is a clear focus by many in industry and government on preparing for a future in which AI is pervasive. CB Insights estimated that over $5 billion US dollars in venture capital financing went to AI startups in 2016, a 62% increase over the previous year.[5] AI presents enormous opportunities to create new jobs, new industries and new ways of connecting.

As AI and automation drive significant structural change across industries, the very nature of work will change. Many existing jobs may be displaced as AI moves beyond monetising user data to changing how products and services are delivered. Adapting to the pace of change will be a major global challenge for the immediate future.

> “
>
> Projects relating to Artificial Intelligence and the Internet of Things have gone a long way in advancing our present technology and making life easier for the average human being.
>
> Internet Society member, Africa

This said, AI systems and technologies could also change the nature of work in a way that empowers workers, diminishing inequality among people and between countries. AI can be a partner in human intelligence, letting us take on and solve much bigger challenges. As one survey respondent explained, “The distance between people’s brains and the Internet will become ever smaller, and the interface between the two ever more sophisticated”.

[5] https://www.cbinsights.com/blog/artificial-intelligence-startup-funding/

> Machine to machine communication increases pressures to cut costs and people are being replaced. This is only going to increase with time. There are economic benefits but also challenges to employment.
>
> Private Sector, Middle East

AI brings potential for huge gains in scientific research, transportation and the delivery of services. If accessibility and open source development win out, AI has the potential to bring dividends to developed and developing countries alike. For example, a country that relies on agricultural production could use AI to analyse crop yields and optimise food production. AI applications in healthcare could be a game changer for disease detection in low income areas.

> Artificial intelligence will be creative destruction. Many jobs will be eliminated by AI, but it can generate new roles and jobs.
>
> Academic, Latin America & Caribbean

But is society itself ready to absorb the change, and are we adequately preparing ourselves for this new economy? For developing economies, new technologies always create possibilities to leapfrog legacy systems, although the infrastructure requirements for AI (and IoT) to be deployed will be significant. The benefits of AI may also be unevenly distributed: for economies that rely on low-skilled labour, automation could challenge their competitive advantage in the global labour market and exacerbate local unemployment challenges, impacting economic development.

The intelligence and services used to manage and implement manufacturing or services may still reside in developed countries rather than being developed locally. AI might exacerbate the digital divide in significant ways that would have geopolitical implications.

> Ensuring Internet technology can create jobs in the market and does not harm the job market is a challenge that has to [be] addressed in the next 5 years and it is an urgent and serious problem internationally.
>
> Government, Asia-Pacific

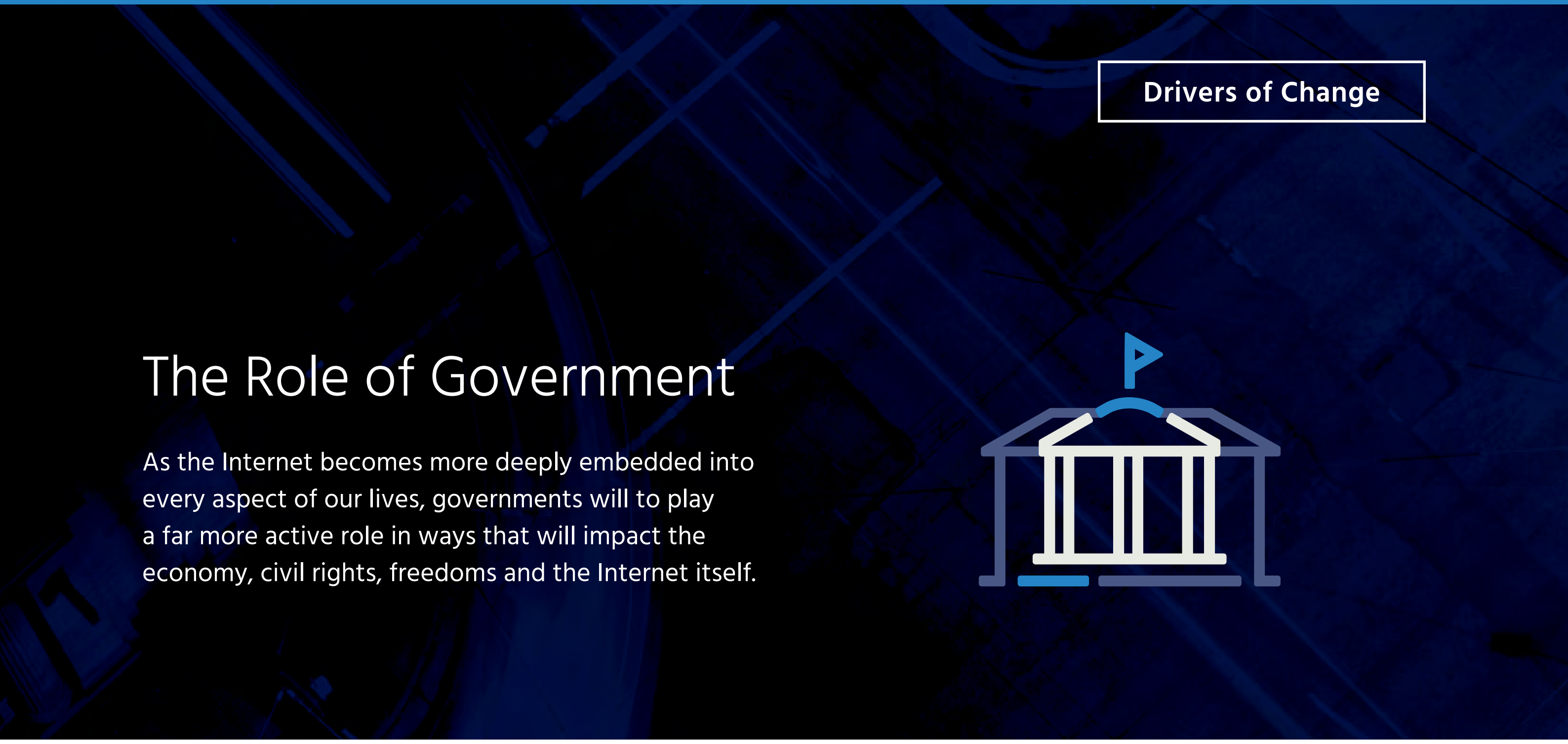
Impact of AI on Internet security and network intelligence

> “
>
> Algorithms are making decisions — and they are making them faster than human decisions, and on our behalf. Furthermore, systems are increasingly opaque. We don’t know where they exist and what decisions they are making …
>
> Technologist, North America

While security and trust will be essential to the future of AI, the technology could also help to address security challenges. As networks and traffic streams become increasingly complex, AI can help network managers to understand traffic patterns and create heuristics that identify security threats. At a basic enterprise level, AI can perform tasks normally carried out by an IT helpdesk, such as troubleshooting employee computer problems. This would give enterprise IT professionals more time to implement security best practices and better secure their systems and networks. Alongside human decision-makers, AI could also sort through the growing mass of security threats online.

AI relies on large amounts of computational resources and data. It is possible that this will drive a redistribution of computing and storage resources and have an impact on Internet architecture. To what degree will there be a need for interoperability and standardisation for AI? And, to what extent are the principles of interoperability, openness and decentralised management of the Internet challenged by the growth of AI?

Related to: Networks, Standards & Interoperability; Cyber Threats



The Role of Government

As the Internet becomes more deeply embedded into every aspect of our lives, governments will to play a far more active role in ways that will impact the economy, civil rights, freedoms and the Internet itself.

Overview

As the Internet expands further into our economy and society, governments will be even more active, both as policymakers and as Internet users themselves. From cybersecurity to societal issues to technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI), governments will face a host of new and complex issues that will challenge all aspects of their decision-making. Technology will increasingly influence the relationship between governments and other stakeholders. As public services and data collection shift to private companies, the roles of the public and private sectors will continue to blur, complicating how citizens hold governments to account. How governments respond to these challenges in the future will impact not only our freedoms, rights and the economy, but also the Internet itself.

Internationally, cybersecurity will drive global governance discussions for the foreseeable future, with the growing risk that governments will limit freedoms or undermine the global nature of the Internet. The Internet will not be immune to the evolving geopolitical tensions driven by nationalism, multilateralism and global power dynamics. How and if states resolve these tensions in the coming years will have tangible implications for the global reach of the technology as well as the overall growth of the Internet economy. To the extent that international cooperation continues in the Internet space, we expect that the tension between multi-stakeholder and multilateral[1] approaches to Internet policy will continue.

> **The future of Internet openness will depend on how governments deal with the growing pressure to respond to security challenges.**

> **New technologies and game-changing business models will force governments to work differently and more inclusively.**

> **Roles and responsibilities in the public and private sectors will continue to blur, creating accountability challenges.**

> **Government policies and structures will be ill-equipped to keep pace with technological developments.**

> **Nationalistic policies will endanger valuable cross border data flows, trigger fragmentation of the network, and silence critical stakeholders.**

[1] In multistakeholder processes, individuals and organisations (stakeholders) from different realms participate alongside each other to share ideas or develop consensus policy. In multilateral systems, several countries and governments work together to solve a particular problem or reach a shared goal.

Government Responses to Future Security Challenges

The scope and complexity of cyberattacks will continue to intensify. Governments will face mounting pressure to act forcefully to protect national security, their citizens and their domestic economies. In fact, our community believes that we are facing a future of increased Internet regulation or legislation.[2]

Yet, policymaking that is reactive and not long term may further fragment the Internet along nation-state boundaries, and also undermine human rights. As the Internet expands into every sector of the economy, the sheer complexity of the security landscape will test even the most sophisticated governments' coordination, capacity and effectiveness. The challenge for developing countries will be even more acute: while Internet Society stakeholders in Africa are confident that their governments see the cybersecurity challenge, they are concerned that governments will lack the skills and capacity to tackle the issues effectively.

Respondents from North America predicted future government reactions to the security challenge to be significantly more drastic than their counterparts in Africa, Asia, and Latin America.[3]

There is a trend today for governments to demand more control over Internet content within their borders in ways that undermine Internet openness, compromise freedoms and rights, and threaten global Internet fragmentation.[4] This could happen in several ways.[5]

Technically, fragmentation will happen if limits are put on the ability of the system to fully interoperate and exchange data packets in an end-to-end way. Governmental fragmentation will happen if states put measures in place that hinder the global reach of the Internet. This scenario could become a reality if governments prioritise short-term national interests — sometimes referred to as "cyber sovereignty" — over longer-term interests and shared responsibility.

[2] Future of the Internet Survey 2 - Question 26: "To what degree do governments regulate or pass laws regarding the Internet"?
[3] Future of the Internet Survey 2 - Question 31: "How extreme are government responses to security risks, challenges, and crises involving the Internet"?
[4] https://www.schneier.com/blog/archives/2013/03/nationalism_on.html
[5] Internet Fragmentation, An Overview, WEF

The Role of Government

Our community believes that government regulations of the future will be more intrusive and restrictive than today.[6]

How governments respond to security challenges will either strengthen people's trust in the Internet or undermine it. In an age of cyberattacks and even cyberwar, some policy makers will sacrifice freedoms and innovation in the name of national security and public order.

> “
>
> The most pessimistic scenario for the future of the global Internet is fragmentation due to nationalistic isolation with highly-filtered access to the Internet.
>
> Technologist, North America

The tension will continue between the need to secure communication for economic and privacy reasons — and governments' need to access those communications for national security. If governments persist in trying to prevent the use of encryption, they put at risk not only freedom of expression, privacy, and user trust, but the future Internet economy as well. Further, interfering with or weakening encryption technologies will create new vulnerabilities and cyber threats.

Our community believes there will be a high degree of acceptance of encryption in the future.[7]

> “
>
> My worst fear is a surveillance state making 1984 resemble a utopia or a glorified cable TV subscription service. One where encryption is banished, anonymous access to the Internet is legally/technically eliminated and the censorship slippery slope continues.
>
> Technical Community, Europe

> “
>
> Nationalism and extremism are shaping the Internet but their influence is disproportionate to the space they occupy.
>
> Civil Society, Middle East

> “
>
> Political views will be expressed more readily online than the traditional way of going out on the streets. Democracy of communications will culminate in greater transparency and accountability of governments.
>
> Government, Africa

> “
>
> Governmental interest in national security will continue to manifest in regulatory actions which inevitably compromise personal privacy and security.
>
> Technologist, Asia-Pacific

Related to: Cyber Threats; Personal Freedoms & Rights

[6] Future of the Internet Survey 2 - Question 27: "How intrusive or restrictive are government regulations or laws on Internet use, services, or operations"?

[7] Future of the Internet Survey 2 - Question 23: "To what degree is the use of encryption and cryptographic technologies on the Internet accepted by society"?

Policy Making in the Digital Age

The sharing of citizens' data between the public and private sectors will continue to grow, as will the blurring of roles and responsibilities between the public and private sectors as the delivery of public services shifts to the private sector. Could this result in the private sector assuming responsibilities that are traditionally those of governments'? If so, will they be subject to the same accountability and governance mechanisms as governments? In the future Internet economy, the use of IoT and artificial intelligence will increase the need to be vigilant about transparency and accountability in decision-making and governance. Transparency and accountability will also be needed to understand and manage an increasingly complicated relationship between the public and private sectors.

> "
>
> The private sector is displacing governments as the locus of policymaking — including in the enjoyment of human rights.
>
> Civil Society, North America

Although cybersecurity concerns will continue to be front and centre, governments will also grapple with IoT and AI. In the face of new technologies, are the existing policy tools able to address the complexity of the challenges ahead? According to our community, policymakers will struggle to keep pace with change in Internet technology in the future.[8]

> "
>
> Technology advances more rapidly than policy and the regulatory environment.
>
> Government, Africa

> "
>
> The speed at which legislation and regulatory frameworks that affects the Internet services can be modified, is an anachronism compared to the technological changes.
>
> Government, Latin America & Caribbean

There will be more pressure on governments to act, even as society struggles to keep up with the pace of change, let alone to consider the long-term implications of today's choices. Governments need to prepare for dramatic changes in the economy, especially in traditional industries most challenged by technology. Government's tendency to apply legacy regulatory models to new and emerging issues is of particular concern.

Whether or not governments chose to take such an approach, the scope of market change driven by dramatic advances in technology will inevitably force a fundamental rethink of existing approaches in competition law and traditional communications regulation. Data will increasingly be seen as an asset linked to competitive advantage, changing the nature of merger reviews, evaluations of dominance and, importantly, consumer protection.

> **Respondents from Africa predict the greatest increase in regulation.**[9]

Governments may turn to multi-stakeholder models of policy development out of necessity, as traditional telecommunications and Internet regulatory approaches are longer seen as fit for purpose.

Related to: The Internet Economy; Personal Freedoms & Rights; The Internet & the Physical World; Artificial Intelligence

[8] Future of the Internet Survey 2 - Question 28: "How intrusive or restrictive are government regulations or laws on Internet use, services or operations"?

[9] Future of the Internet Survey 2 - Question 26: "To what degree do governments regulate or pass laws regarding the Internet"?

Multistakeholderism and Multilateralism and the setting of global norms

Will governments embrace globalisation, or will they respond to domestic pressures to strengthen both physical and cyber borders? Will they support and promote multistakeholder approaches to policy, or will they retrench behind the walls of multilateralism? The rise of nationalism and populism around the globe could cause governments build national policy barriers that fragment the Internet. If current trends are any indication, more and more governments will restrict and control Internet use and access through censorship, network shutdowns and other means.[10]

All stakeholder groups and regions saw significant policy and regulatory differences between nations today; however, respondents also saw a trend toward global compatibility — although they were uncertain about the final outcome.[11]

At the same time, governments could become more attuned to the need for cross-border and cross-sector cooperation on cyber threats like crime and terrorism. The complexity of the challenges should compel governments to work with other stakeholders.

[10] https://freedomhouse.org/report/freedom-net/freedom-net-2016

[11] Future of the Internet Survey 2 - Question 25: “Are national Internet policies and regulatory frameworks globally compatible or are there strong differences along national or regional lines”?

However, for such efforts to work and to have legitimacy, they will need to move beyond traditional public-private partnerships and include civil society.

Multistakeholder approaches will continue to receive measured support from *some* governments, particularly when it comes to setting norms and best practices for cyberspace. But political change is slow, and the tension between multilateralism and multistakeholderism will continue for the foreseeable future.

> "
>
> The legal tools available to address cyberattacks have limited teeth and lack the ability to prosecute. There will be a need to review existing laws to strengthen the legal framework in dealing with emerging cybercrimes.
>
> Technologist, Latin America & Caribbean

> "
>
> Fragmentation of the Internet will occur without coordination of multistakeholder and governance mechanisms.
>
> Technologist, Latin America & Caribbean

While our community is optimistic, predicting more use of multi-stakeholder approaches in the future,[12] they also question whether civil society groups and activists will have a real seat at the table. The answer to this question will have significant implications for the future of online rights and freedoms.

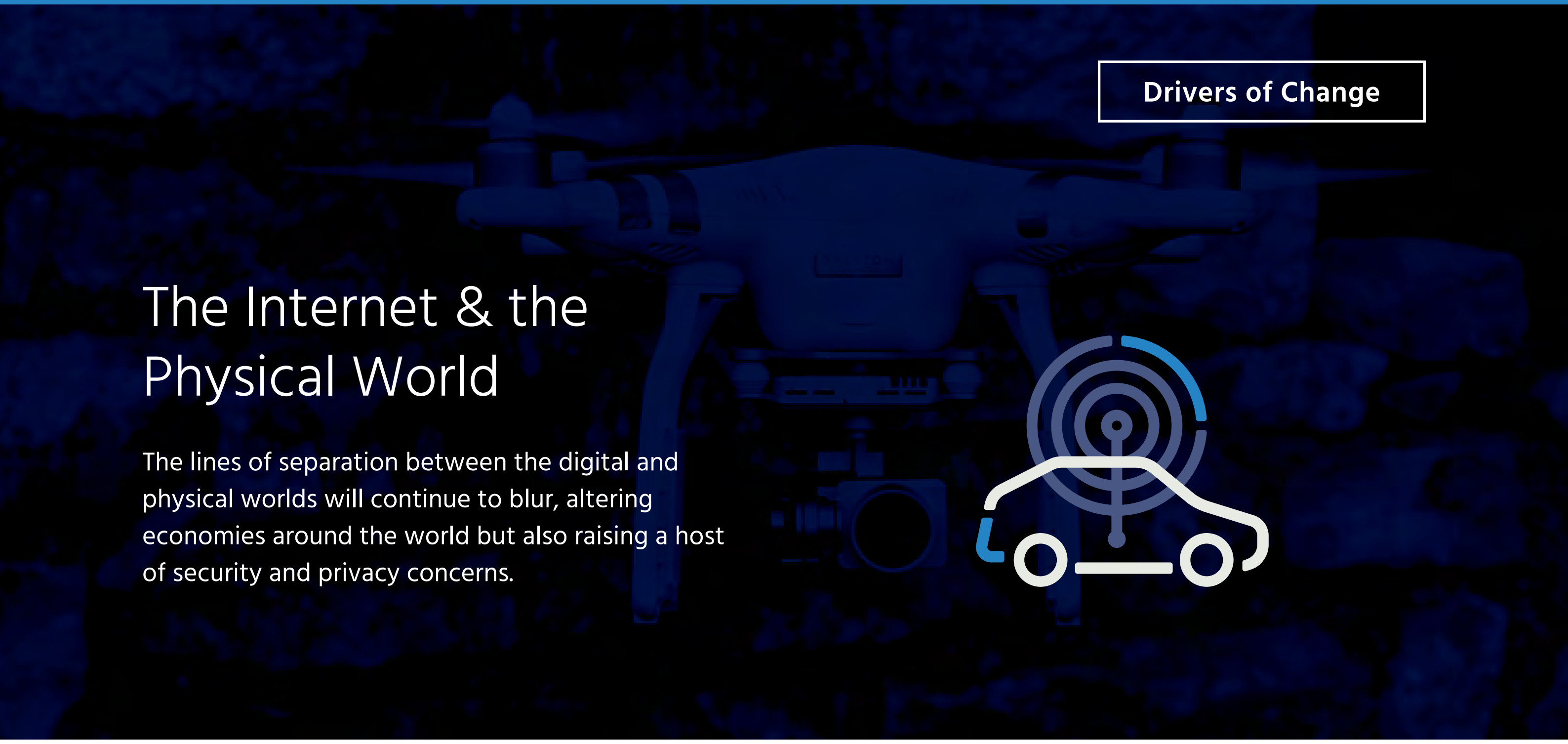
> "
>
> It is essential to radically strengthen users and civil society powers in the multistakeholder model to compensate for the relative decline of direct governmental influence.
>
> Government, Europe

Will we see new models of Internet governance in an evolving multipolar world? How will these diverging models and the rise of new powers shape the global Internet and its core principles? If the international system continues to turn inwards, the implications for the *global* Internet will become ever more profound.

> "
>
> I am concerned with an increased consolidation in businesses, government positions and Internet governance resulting in alliances to preserve the status quo.
>
> Technologist, Latin America & Caribbean

Related to: The Internet Economy; Cyber Threats; Networks, Standards & Interoperability

[12] Future of the Internet Survey 2 - Question 29: "Are major decisions on Internet governance and policy made primarily through multistakeholder approaches or more strongly by national governments or multilateral approaches"?



The Internet & the Physical World

The lines of separation between the digital and physical worlds will continue to blur, altering economies around the world but also raising a host of security and privacy concerns.

Overview

The Internet of Things (IoT) is removing the separation between the Internet and our physical world. Gartner predicts that 8.4 billion “things” will be connected in 2017, more than doubling to over 20 billion by 2020.[1] IoT itself is not new, but the combination of increasing bandwidth, sensor technology and Artificial Intelligence (AI) may trigger an explosion of ubiquitous connectivity. Virtually everything that can be connected will be connected. This will transform whole economies and societies.

While innovation brings opportunity, the shift to a hyperconnected world raises key questions and uncertainties for the future. As the Internet will be used to control objects, infrastructure and much of our environment, questions about privacy, interoperability, regulation and security will need to be urgently answered.

The convergence of the physical and digital worlds will fundamentally change what it means to be online — this will have far-reaching implications for society and all sectors of the economy, from medicine to manufacturing.

For IoT to thrive, the security of connected devices must be addressed.

If appropriate safeguards to ensure transparency and user control are not put in place IoT could drive data-collection and use in ways that further undermine privacy and deepen surveillance.

Interoperability will be essential to the overall success of IoT and to maximise its positive impact on the global economy.

[1] Gartner source: http://www.gartner.com/newsroom/id/3598917

Socioeconomic Implications of Converging Digital and Physical Worlds

When virtually any object can be connected to the Internet, our digital and physical worlds will increasingly converge. IoT forms the basis of this convergence, but IoT is not a single technology. It is a set of applications and capabilities, services, and infrastructure that provide the intelligence needed to make connected objects useful. Developments in artificial intelligence will enable new means of interacting with connected objects through voice or gesture, and virtual and augmented reality will be powered by data generated by IoT. With IoT and AI, as well as increased bandwidth and sensor technologies, we are approaching a state of convergence where the lines between the digital and the physical blur. But for all of this to happen, we will need ubiquitous, reliable and secure connectivity around the globe.

> “
>
> We are entering a new phase of technological evolution, a phase where the Internet will be fully integrated into every part of our lives — how we learn, how we work, how we shop, how we get around.
>
> Private Sector, Europe

IoT could bring about a world in which the Internet is fully integrated into every part of economy and society. It may reduce mundane tasks, freeing workers to focus on creative, non-routine aspects of their jobs. But, as convergence gains momentum, every industry faces disruption that may change or even destroy jobs.

> “
>
> The Internet of Things, virtual reality, and artificial intelligence are changing the nature of work in a way that would empower and liberate people, and diminish inequalities among people and among countries -- or the outcome could be a diametrically opposite one.
>
> Academic, Europe

IoT also brings a convergence of digital and analogue industries, for example, of technology and manufacturing firms. The Internet will evolve from being dominated by the Web and mobile applications to an Internet that permeates all aspects of the physical world. This will change current market dynamics and bring increasing competition between traditional industry and the ICT sector.

The industry-specific regulatory frameworks we currently have in place are not well suited to a world in which connectivity blurs the lines between sectors of the economy. The challenge for policymakers will be twofold: one, to avoid falling further behind technological change; and two, to avoid disproportionate and potentially harmful regulations in response to evolving security threats.

> “
>
> Countries need to enhance their industrial policies and consumer protection-frameworks to prepare for IoT ... National IoT frameworks will also need to incorporate cultural considerations that will impact IoT development.
>
> Internet Society Member, Africa

While lives may be improved by smart homes and smart cities, IoT's promise of billions of devices constantly transmitting data raises many issues. We may see increased mass surveillance, the further erosion of privacy, and a growing dependence on data collection, analytics, and curation. The implications for privacy are profound. Without essential safeguards, greater amounts of data will be collected and used without the user's knowledge or control.

> “
>
> IoT will make what remains of us, in terms of privacy, publicly available and 'published'.
>
> Technologist, Middle East

Related to: Artificial Intelligence; The Role of Government; The Internet Economy

The Pressing Need for IoT Security

Connected devices add enormous complexity to an already complex security environment. They also raise the stakes, with increased potential for cyber threats to damage physical assets and harm human life. We are adopting IoT faster than we can secure it. This rush is accelerated by the increasing number of new entrants and the push to quickly release Internet-connected devices produced without prioritising security.

> “
>
> Africa must develop agriculture, AI, and IoT together to respond to Africa-specific challenges instead of copying others. However, it will be necessary to assure a greater level of security as attacks become more and more numerous.
>
> Internet Society Member, Africa

The Mirai attack of 2016[2] starkly shows the effect plug-and-play and remotely-managed IoT devices can have on the broader Internet. Many of the connected devices on the market today have very limited built-in security measures and will not be updated through the devices’ anticipated lifetime. This explosion in the number of connected devices — in transportation, wearables, health, smart homes, and alarm systems — alters the cyber threat landscape in unprecedented ways. A lack of agreement on IoT Security frameworks and best practices may jeopardise the safety of individuals around the globe.

[2] https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

> “
>
> IoT compounds every security problem ever seen and multiplies every problem of the Internet. Your toaster could be sending out spam.
>
> Technologist, North America

Will governments increase regulation of the Internet in response to this new threat landscape? If so, will their responses be effective and respectful of privacy and individual autonomy? The more risk there is to critical infrastructure, the greater the perceived need for governments to intervene. If threats to critical infrastructure stem from something as innocuous as unsecured Internet-connected light bulbs, governments may be tempted to regulate in very detailed and prescriptive ways.

All stakeholders, from users to manufacturers to governments, will need to be more security aware and work together towards a more comprehensive and resilient security environment. The insurance industry may exert market influence, for example, by requiring systems or devices to have security certifications in order for their owners to be insurable.

A sustainable and effective long-term solution will require ongoing collaboration, and a commitment by manufacturers and service providers to incorporate privacy and security in their design processes, from initial conception to long-term support and updates. We need to address IoT-related security issues before we can realise the full benefits of the Internet economy.

> “
>
> Security and trust of the consumer will be the key. With the current technology it is impossible to embed security. Governments worry about this. It is important to have security to have the full potential of the Internet. Security and trust are critical; the public and private sectors should work together. There should be a standard. It’s a government challenge.
>
> Government, Asia-Pacific

Related to: Cyber Threats; The Role of Government

IoT, Interoperability and the Future of Internet

Interoperability is fundamental to the success of IoT. Much of IoT's promise is based on the assumption that everything falls into a common structure, with systems and data that are interoperable. McKinsey & Company estimates that "40 percent of the total value that can be unlocked requires different IoT systems to work together".[3] This won't just happen by itself. If IoT standards and Application Programming Interfaces [4] (APIs) are proprietary, especially in the early days of product development, we may not be able to optimise network infrastructure and spur innovation. As Jari Arkko, former IETF Chair put it, "Without interoperability, lights won't work with the switches, sensors can't be read by your smartphone, and devices cannot use the networks around them".[5] As one technologist in Asia predicted, "there may be a certain period of time in which the Internet infrastructure built for IoT will not be optimised due to the lack of interoperability between IoT systems".

> "
>
> Everyone loves a networked toaster! But interoperability and security becomes major factors… at least for technologists. Consumers won't care…
>
> Technologist, North America

Interoperability, standards and protocols, and security are all intertwined and essential to the success of IoT. Without them, we face a different kind of fragmentation — where devices and systems simply will not work together. People will hesitate to adopt IoT if it cannot be integrated with other technologies, it is too complex to easily manage, or if they risk being "locked in" to a particular vendor.[6]

> "
>
> The pressure to be a leader will mean that companies will rush to bring more and more IoT devices using proprietary/non-standard technologies. To mainstream these IoT devices on the Internet will require localised gateways that can integrate and bridge between the proprietary technologies/devices and the Internet. The proliferation of gateways/bridges between proprietary technology driven IoT devices and the rest of the open, end-to-end Internet, will present new Interoperability challenges to the Internet.
>
> Technologist, Middle East

Iot will make unprecedented demands on communication infrastructure and data storage, requiring significant investments to ensure security and privacy. In some cases, specialised access networks may need to be built to support sensors, for example in smart cities. This will increase demand on networks, energy supply and for Internet addressing. For IoT to work, the migration to IPv6[7] needs to happen, and quickly.

> **Our community is optimistic about ISPs' future ability to supply bandwidth to meet increasing demands. In fact, respondents from Central America, Western Africa, Indian Ocean Islands and the Middle East are confident that today's deficit will shift to a surplus over the next five years.[8]**

Related to: Networks, Standards & Interoperability; The Internet Economy

[3] http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

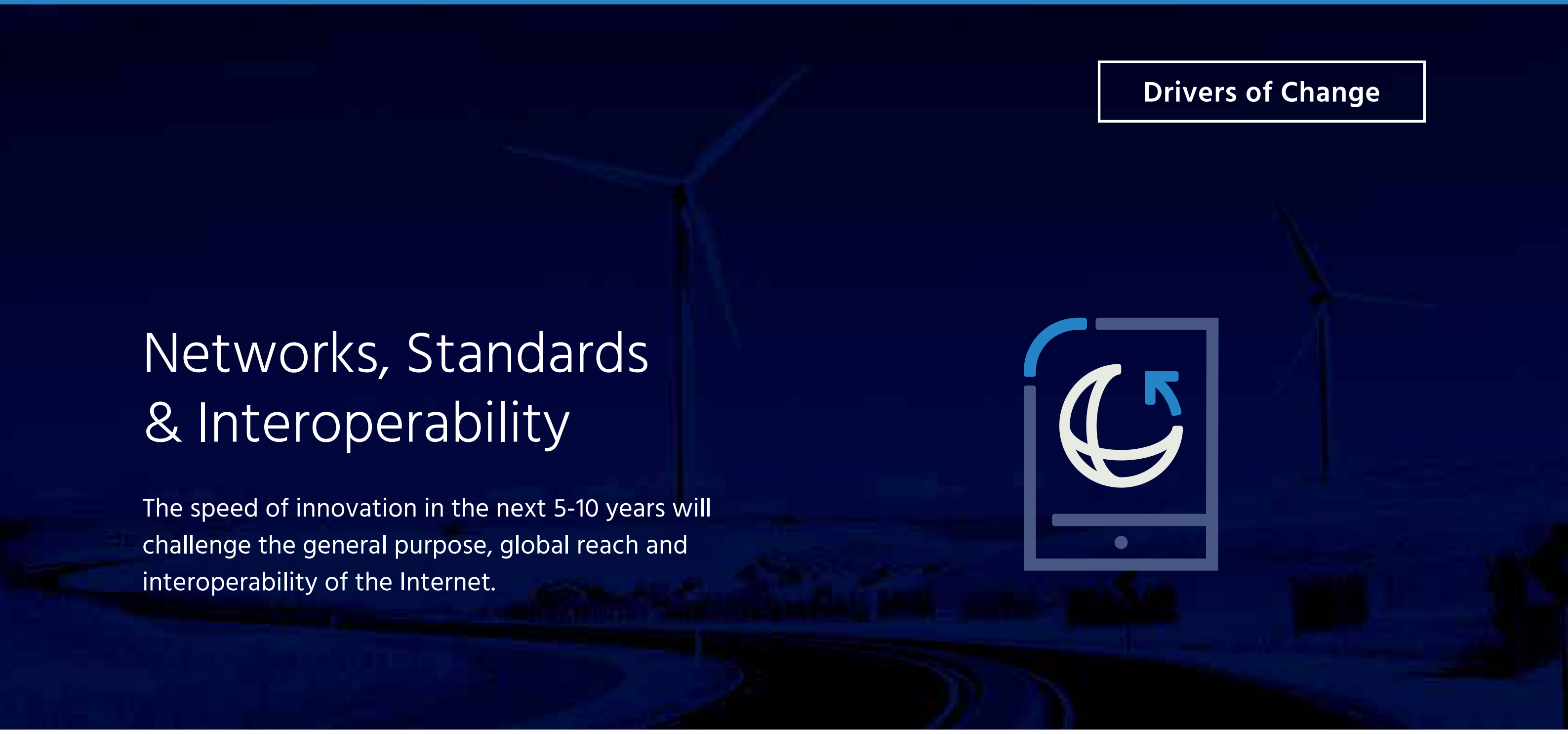
[4] An application programming interface (API) is a set of protocols, routines, functions and/or commands that programmers use to develop software or facilitate interaction between distinct systems. Source: https://www.techopedia.com/definition/24407/application-programming-interface-api

[5] Jari Arkko, https://www.ietf.org/blog/2016/01/an-interoperable-internet-of-things/

[6] https://www.internetsociety.org/doc/iot-overview

[7] https://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6

[8] Future of the Internet Survey 2 - Question 2: "How well are Internet service providers (ISPs) able to meet the demand for bandwidth in [RESPONDENT'S REGION]"?



Networks, Standards & Interoperability

The speed of innovation in the next 5-10 years will challenge the general purpose, global reach and interoperability of the Internet.

Overview

The Internet has always evolved, both in its technologies and how we use it. The standards that define its shared protocols also change, and produce freely available specifications. Yet, these same standards will be challenged in the future by the sheer speed of innovation.

As the Internet has evolved and grown — with some parts optimised for certain traffic patterns or expected uses — it has always retained several key properties including general purpose, global reach and interoperability, and absence of central authority.[1] This notion of general purpose means that the Internet is not designed for just one application, but as a general infrastructure on which new applications could be conceived — without permission.[2] As wireless platforms become the access technologies of the future, these basic properties of the Internet will be under pressure.

This "general purpose" Internet is facing three growing pressures: ubiquitous connectivity; significant changes at the edge of the network (including the devices and applications that generate and use traffic); and the decline of traffic that is passed between backbone networks operated by different entities.

Taken together, the evolving edge, the dominance of wireless access, and the decline in transit may put pressure on the general-purpose, open Internet and its ability to support ongoing evolution and innovation. These developments demand attention to ensure they do not create conditions that forestall industry competition and reduce the choices and opportunities available to Internet users.

> **The proliferation of connected systems and wireless devices will bring ubiquitous connectivity, letting users roam seamlessly across networks, without even being aware of it.**

> **The network edge will become more complex, with many and varied devices connecting to new services using specialised networks. These new technologies and services — such as IoT — are reshaping and putting pressures on the general-purpose Internet.**

> **The nature of transit will change due to the increasing use of Content Delivery Networks (CDNs), caching and other specialised services that flatten the network hierarchy. This may lead to reduced competition and lack of innovation in the core of the network.**

> **Increasingly, developers are relying on proprietary standards which will be a barrier to innovation and interoperability. Open standards development will need to evolve to ensure standards are still relevant in a world of competing proprietary systems.**

[1] https://www.internetsociety.org/internet-invariants-what-really-matters
[2] http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

Ubiquitous Connectivity

Mobile access is already the primary way people connect to the Internet in many parts of the world. Emerging technologies and use cases promise to accelerate that trend. Devices that hop seamlessly from WiFi to cellular networks, and technologies such as 5G, will be optimised for uses that put a premium on continuous connectivity no matter where we are. Connected systems and devices — such as actuators and sensors — that comprise the mushrooming Internet of Things (IoT), will increase the number of connections and demand for bandwidth. At the same time, increases in bandwidth will spur the deployment of HD and 4K video, and encourage new uses that have yet to be imagined.

> **Overall, our community sees the future trending towards ISPs being able to better meet the bandwidth demands of their users.[3]**

> Connectivity and ubiquitous coverage are the backbone of an inclusive new digital world and a prerequisite for a successful further innovation of services online.
>
> Private Sector, Europe

These increases in scope and scale follow well-established patterns of Internet growth. From an end-user perspective, ubiquitous and increasingly robust connectivity will simply be part of the environment most of the time and for many people. Increasingly, the state of being *offline* will be the exception and may need to be actively sought out.

The future of ubiquitous connectivity is not without challenges. For people to roam seamlessly across different wireless technologies, we will need continued development and deployment of open standards that facilitate interoperability. To ensure that the Internet remains an open, global communications system, network operators will need to stay committed to deploying of core technologies (e.g., IPv6) and best operational practices.

> Will I still be seeking out wireless zones, or having to tote around my own hotspot?
>
> Technologist, North America

Related to: The Internet & the Physical World; The Internet Economy; Digital Divides

[3] Future of the Internet Survey 2 - Question 2: "How well are Internet service providers (ISPs) able to meet the demand for bandwidth in [RESPONDENT'S REGION]"?

Evolution of the Edge

Broadly defined, the edge of the Internet includes both the networks and devices within homes and enterprises, as well as the Internet service provider networks that connect those homes and enterprises to the global Internet. The Internet was originally conceived as an end-to-end network connecting peer devices, but services are emerging that are delivered by finely-tuned infrastructure that includes specialised networks and purpose-built services made available via those networks. This evolving edge is rapidly changing how individuals interact with the Internet. It offers the potential of new and exciting interactive applications and services, but also raises challenges for the current general purpose architecture of the Internet.

> “
>
> The Internet will change from end-to-end to edge-to-edge.
>
> Technologist, Europe

Home networks are supporting a growing number of services that extend far beyond the home and the traditional edge of the network. For example, an individual’s home appliances can participate as part of the regional electric power management system. Health devices in the home can be connected into remote health monitoring systems. Entertainment and personal application data can be stored remotely and accessed seamlessly on demand. These systems are completely independent of each other while using the same underlying network infrastructure of the home. We are only at the cusp of what this new networked environment will mean for innovation and new services.

> “
>
> The proliferation of “private” IP-based networks that don’t use the “public Internet” is going to increase by orders of magnitude. Real-time and other applications (voice, video etc.) are latency intolerant and need a certain quality of service. Think “all bits are created equal, but some bits are more equal than others”. Unless the “public Internet” can incorporate and adapt to other use and applications, private networks (IP networks that are not end to end and don’t use BGP or DNS) will continue to be deployed — and its already happening.
>
> Technologist, North America

These new services are changing what we traditionally considered to be the edge of the network. They often run on special hardware, and are typically delivered using cloud infrastructures and CDNs connected via customised connections. Connected sensors or devices, part of the IoT, make use of intermediary hubs or proprietary protocols. They are also tied to dedicated back-end services rather than being individually addressable on the network. This evolving edge, and its growing complexity of specialised networks and purpose-built services, may create independent islands of connectivity. This could lead to fragmentation of the open, global Internet. If specialised networks dominate the connectivity environment, this will create obstacles for innovation and the deployment of new services and technologies.

> “
> Parastatals (and normal businesses) try to protect their IT infrastructure at the perimeter but BYOD is interfering with their ability to do so and many networks have become porous as a result.
>
> Internet Society Member, Africa

> “
> Businesses want to protect their business models as much as possible — they want to use TCP/IP but not the “public Internet”. Instead, they are establishing private networks and private domains to create control for their own business structures.
>
> Technologist, Asia-Pacific

Related to: The Internet & the Physical World; The Internet Economy

Decline of Transit

Complementary to the evolving network edge, the traditional hierarchy of backbone, access and enterprise networks is flattening. In the past, this hierarchy meant that backbone networks would exchange, or transit, traffic destined for access networks they did not directly connect. However, the increasing use of CDNs and the continuous growth of Internet Exchange Points (IXPs), where traffic is often passed directly to access networks, have reduced the need for transit traffic. Geoff Huston, Chief Scientist at APNIC, referred to this as "the death of transit".[4]

> There is going to be a gradual scaling up of networks to carry the increasing traffic being generated by users, especially video content.
>
> Government, Africa

While these changes improve performance — by reducing latency and jitter — for end-users and lower costs for large-scale service providers, the cost of implementing capabilities such as CDNs and other close-to-the-edge service points puts smaller or emerging service providers at a disadvantage. For example, large on-demand video providers can establish caches close to their users to provide better quality service. This trend may lead to consolidation and reduced competition in service offerings.

The potential implications include reduced innovation in long haul networks and lack of choice for consumers. Ensuring a healthy competitive ecosystem is crucial to ensure that we have the necessary infrastructure for the next generation of permissionless innovation.

> **Respondents from Africa and Asia reported a significant trend toward greater use of the global, public internet, while respondents from Europe and North America see a significant trend toward greater use of closed, access-limited, or private IP networks.**[5]

Related to: The Internet Economy

[4] Geoff Huston, APNIC, is widely credited for identifying the "death of transit" and its implications for the global architecture of the Internet. https://blog.apnic.net/2016/10/28/the-death-of-transit/

[5] Future of the Internet Survey 2 - Question 36: "To what extent are private or closed Internet Protocol-based networks being deployed or used for services in contrast to IP-based networks that are fully connected to the global, "public" Internet"?

Innovation and Standardisation

Open and voluntary standards have long been at the core of the Internet's success. They will, however, be challenged in the future by the speed of Internet innovation, the complexity of the emerging infrastructure and services, and the emergence of proprietary systems and walled gardens. Standards development processes are also under increasing threat from companies that can use their powerful market presence to create de facto standards, bypassing open standards processes and risking fragmentation.

> “
>
> Optimistically the (so-called) “Internet of Things” (so-called) will have faded in significance, as the Internet itself simply continues to expand with increasing numbers and varieties of connected devices. Successful manufacturers of these devices will have embraced the Internet ecosystem, in terms of open standards, Internet best practices, and appropriate measures to ensure security and longevity of their devices.
>
> Technologist, Asia-Pacific

Established approaches to formulating Internet standards must evolve if they are to remain relevant going forward. Simply put, the challenge for established standards organisations and processes includes engaging the innovators who either do not see the benefits of standardisation, or for whom the process of standardisation is too cumbersome.

Related to: The Internet & the Physical World; The Internet Economy

Cyber Threats

The scope and severity of global cyber threats and how we respond to it will have far-reaching consequences for the future of the Internet.

Overview

“Attacks against businesses and nations hit the headlines with such regularity that we’ve become numb to the sheer volume and acceleration of cyber threats”.[1] And yet, as our dependence on the Internet continues to increase, the scope and severity of security challenges and vulnerabilities will only intensify. Cybersecurity will be the most pressing challenge of the next decade; responses to date have been thoroughly insufficient and the costs are escalating.

Cyberattacks and cybercrime will shape the Internet and our relationship to it. Inadequate management of cyber threats will put users increasingly at risk, undermine trust in the Internet and jeopardise its ability to act as a driver for economic and social innovation. Misinformed or disproportionate government responses will threaten freedoms, and contribute to a climate of fear and uncertainty. How we respond to increasing cyberattacks and cybercrime is a fundamental question — the answer will largely determine the future of the Internet.

The continued growth of the Internet will depend on how we collectively respond to the volume and scale of cyber threats.

As governments come under pressure to respond to cyber threats, there is the very real risk that online freedoms and global connectivity will take a back seat to national security.

New accountability, incentive and liability models are urgently needed not only to increase cybersecurity readiness and reduce vulnerabilities but also to ensure end-user security.

The complexity and scope of cyberattacks necessitates multistakeholder and expertise-driven responses for the digital economy to thrive and for trust in the Internet to be rebuilt.

[1] 2016 Norton Cyber Security Insights Report https://us.norton.com/cyber-security-insights

An Increasing Range of Cyber Threats

The scale of cyberattacks is steadily growing, and many anticipate the likelihood of catastrophic cyberattacks in the future. We already see attacks on a national scale, so it is not farfetched to imagine a digital pandemic with attacks crippling entire economies. As one North American industry analyst put it, a "digital Pearl Harbor is coming …"

As the Internet becomes intertwined with national security, cyber offense and defense strategies will shape the future Internet for industry and individual users alike. Cyberspace is now considered the fifth domain of warfare[2], but there are few agreed rules of engagement.

The threat of destructive cyber conflict will only increase over the next decade. Conflicts will be initiated not only by nation states, but also by their surrogates, and by independent political movements and private actors. Acts of cyber conflict will be coupled with disinformation and propaganda to destabilise states and economies. Recent cyberattacks that appear to be designed to destabilise political systems are especially alarming and point to a future in which undermining governance structures, and therefore the values that they stand, for will become more commonplace.

[2] http://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html

Cyber Threats

> “
>
> [In response to the growing threat of cyberattacks], governments attach increased importance to issues of cybersecurity and are strengthening the adoption of various protective measures such as technology, policy, and enhancing international cooperation.
>
> Technologist, Asia-Pacific

> “
>
> I am worried about the attempts to use 20th-century regulatory frameworks to address 21st-century internet issues.
>
> Civil Society, Latin America & Caribbean

As the digital network becomes intertwined with everything from lights bulbs to health care to cars, users are increasingly vulnerable to cyberattacks. Today’s narrow approach to critical infrastructure protection will be ineffective in a hyperconnected society and economy where all digital infrastructure will be critical.

> “
>
> I think the government will hire white hat hackers or attract hackers to become white hat hackers.
>
> Internet Society Member, Middle East

Business models will depend more and more on data sources and on interconnected data and its analysis, creating more attack vectors. If “data is the new oil”,[3] the growing market for hacking and data theft puts the foundation of our future economy at risk.

For the open Internet to continue as a platform for social and economic growth, users must be able to trust that the government agencies and businesses collecting and using their data are resilient and will address cybersecurity threats adequately.

> “
>
> There are too many business models at the moment that revolve around the collection and “mining” of data, with no understanding on how that data will be kept safe, especially once it becomes stale or the entity that collected it runs out of money. Public administrations are no exception and may actually end up being the easier target.
>
> Technologist, Europe

Related to: The Role of Government; The Internet & the Physical World; The Internet Economy

[3] http://fortune.com/2016/07/11/data-oil-brainstorm-tech/

Inadequacy of Responses and the Impact on Trust

From hacking networks to steal personal information, such as financial details and passwords, to security breaches that affect the physical world, and attacks that impact democratic processes, the growing scope of cyberattacks means that all of society is at risk, not just those online. Cyber threats are not only undermining trust in the Internet, but also in the institutions and political processes that citizens depend on.

> **While all stakeholders and regions believe that the benefits of the Internet will continue to outweigh the risks, there is an overall perception that risks are increasing.[4]**

> "
>
> There hasn't been an "Internet Off Day" Movement yet. The trend will be to continue to use the Internet despite the concerns over trust.
>
> Private Sector, Europe

All our survey respondents, across stakeholder-groups and regions, expect to see high investment and innovation in Internet security in the future. This accords with the view of Gartner Research, who forecast that $92 billion will be spent on cybersecurity in 2017, and over $113 billion in 2020.[5] However, if stakeholders fail to collaborate together, this investment will fall short of the challenge.

> "
>
> In an ideal world, digital security becomes the basis of everything and the idea takes off — and people get it… security for network, users, data, infrastructure is interrelated and all part of national security. People who think more deeply and broadly about security get it — get it — that you can't undermine security in a small case without impacting the big picture.
>
> Academic, North America

Neither government nor the private sector can deal with the scope and scale of cyber threats alone. Due to the interconnected nature of the Internet, lone actions by stakeholders, although necessary, will do little to mitigate or eliminate cyber threats. Driven by the need to be seen to be "doing something" in the face of ever-bolder cyberattacks, we expect that government responses to cybersecurity challenges will be increasingly reactive. However, such responses may not effectively mitigate the threat and will likely result in disproportionate over-regulation. Effective action and building network resilience towards cyber threats will only come through information sharing, strategic thinking and collaborative efforts among stakeholders.

> "
>
> If we are not able to combat these threats we are going to face a pessimistic future.
>
> Technologist, Africa

[4] Future of the Internet Survey 2 - Question 20: "To what extent do people see a tradeoff between the social and economic benefits of the Internet versus potential security and social risks posed by the Internet"?

[5] http://www.gartner.com/newsroom/id/3638017

Cyber Threats

The way stakeholders adapt to future cyberattacks could change the Internet from an open and collaborative Internet to a fragmented, closed but "secure" network environment. A fundamental change to the architecture and underlying principles of the Internet could deliver a dystopian future of secure walled gardens, filtered access and total user visibility (no encryption, anonymity or privacy).[6]

> There's lots of talk surrounding security and encryption, but users aren't willing to use anything that's even slightly inconvenient. I suspect in five years we'll still be talking about how important security is, and things will be even more insecure.
>
> Technologist, Africa

In such a world, the interests of national security will overshadow freedoms and rights. Whatever happens, we expect the tussle between perceived national security interests and end-user security measures (e.g., encryption) to continue.

> The outcomes from the clash between security and privacy are not at all certain. Encryption may be outlawed in a number of countries just as it is embraced in others and the implications for cross-border data flow are potentially quite enormous and harmful.
>
> Private Sector, Europe

[6] It's important to note that this drive toward walled gardens could come through a security lens and not, as typically expected, through lack of competition [community data result].

Any dilution or denial of freedoms and rights will undermine trust in the Internet and its ability to drive economic and social innovation.

> “
> I’m afraid that governments will, under the pretext of protecting their national security and sovereignty, censure more and more and cut off the Internet ever more often. We will end with a different Internet controlled by the governments in each country.
>
> Civil Society, Africa

There is a realistic alternative to the dystopian vision of closed networks. If, when faced with cyber threats, stakeholders respond constructively with coordinated responses to cyber incidents, mutual cooperation on cybercrime, convening multistakeholder platforms to better collaborate on national cybersecurity strategies, and ensuring respect for human rights, then cyber risks can be better managed and mitigated, and trust restored.

Technical advances may also result from the threat and impact of cyberattacks and cybercrime. For instance, past advances in encryption technologies have given users more secure devices and services that let them perform more sensitive activities online. As one technologist noted, “the negative trend is the increase in cybercriminal activity. The positive trend is our ability to build more kinds of devices and protocols that will make it harder”.

> “
> [There is a] need for DNSSEC, as well as new standards like DANE & Strict Transport Security (STS) plus whatever else is needed to prevent malware from being distributed and to keep spam in emails in check. I believe that the new technologies will actually make the Internet safer and keep it operating in a stable manner.
>
> Government, Europe

Related to: The Role of Government; Personal Freedoms & Rights; Networks, Standards & Interoperability; The Internet Economy

New Responses and New Models

Work to develop norms of behaviour, legal frameworks, or even treaties will accelerate over the coming years, as governments try to address the dizzying array of challenges in cyberspace. The pressure to put “rules of the road” in place will continue, but it is unclear whether governments will prioritise cross-border cooperation over national sovereignty and security. And, crucially, would treaties or norms actually curb harmful behaviour by governments or private entities, or would they simply be for show — to be perceived to be “doing something”?

> “
>
> A lack of a national and international body of law will allow crime and abuse to run rampant.
>
> Technologist, North America

The long-discussed need for a global culture of cybersecurity will take on new relevance and urgency, as cybersecurity becomes the responsibility of everyone. From financial markets to elections to health care provision, no system will be immune to cyberattacks and cybercrime in the future. The idea that “the network is only as strong as its weakest link” takes on new meaning in a hyperconnected world, where an individual’s connected devices could undermine critical infrastructure. The Dyn attack in 2016 demonstrated how a simple connected device can be used as part of a botnet to attack critical infrastructure.[7]

New security baselines, along with accountability and incentive models will be essential as we move forward. It will become even more urgent to increase security literacy and build security into connected devices. A market for security needs to be created to ensure greater network and device security — for example, liability models may emerge that extract damages from those who undermine the network through device vulnerabilities or malicious action. Government procurement practices will need to incentivise security.

In a networked world of increasing vulnerability to cyberattacks, cyber governance can no longer remain solely in the hands of governments. Indeed, much of the global Internet infrastructure is developed, owned and maintained by the private sector. The complexity and scope of cyberattacks means governments acting alone will not be able to provide the inclusive and expertise-driven regulatory responses we will need.

> “
>
> The other uncertain prospect is the use of cyber arms and cyberwars to achieve political gains between major powers. This is already happening but it is uncertain whether it will lead to major disruptions to the network and perhaps reduce confidence by Internet users in it.
>
> Academic, Middle East

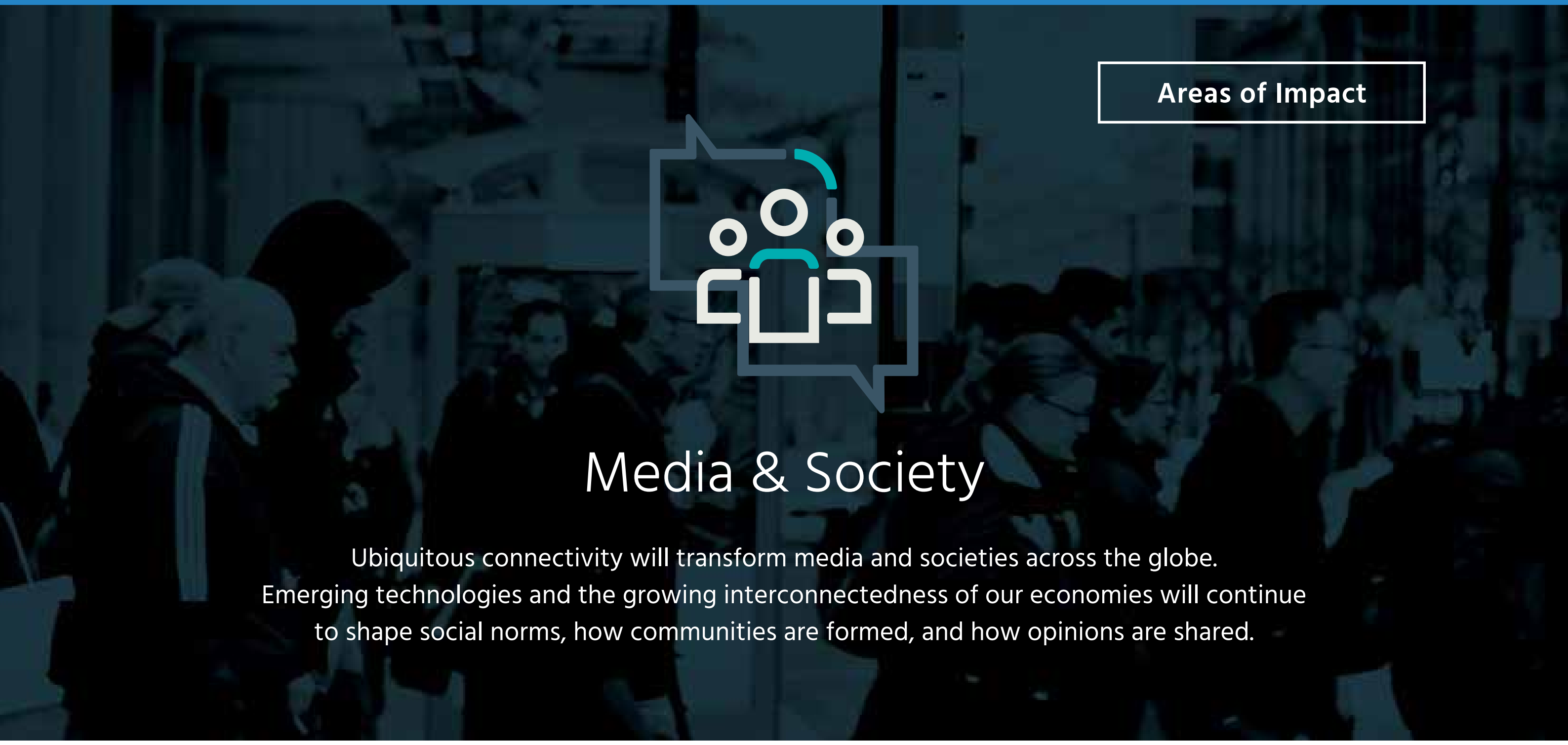
There is no easy fix to the threat of cyberattacks and cybercrime. The Internet’s characteristics of openness, global reach and permissionless innovation are foundational to the technology’s success. Yet these same characteristics make it easier and less costly to launch cyberattacks, presenting a formidable challenge for the future.

Related to: The Internet & the Physical World; The Role of Government; The Internet Economy

[7] The 2016 Dyn attack saw a botnet (a controlled network of devices) used to attack the domain name service provider Dyn. The attack, carried out by a large number of infected IoT devices, caused some Internet platforms and services to be unreachable by parts of the Internet.

7

Areas of Impact



Media & Society

Ubiquitous connectivity will transform media and societies across the globe. Emerging technologies and the growing interconnectedness of our economies will continue to shape social norms, how communities are formed, and how opinions are shared.

Efforts to develop online social norms or to address violent extremism online will challenge certain tenents of the Internet, namely, anonymity, privacy and free expression.

Automation-driven changes to the labor market will cause considerable anxiety in the short term as people worry about the future of work and whether they have the skills to succeed in the new economy.

The changing media ecosystem is democratising access to information while also raising concerns about the implications of fake news and disinformation for public discourse.

The data-driven economy will blur the lines between the public and private sectors, creating challenges for accountability and transparency. Government policies and processes could chip away at the global Internet and lead to its fragmentation.

Overview

As the Internet integrates itself further into all aspects of our daily lives, it will affect how we work, communicate and govern ourselves. It has a tremendous ability to connect disparate groups around the globe to each other and to an astounding amount of information. In fact, Cisco estimates that global IP traffic will increase by 300 per cent over the next five years, and that it will reach 3.3 zettabytes (2^{70} bytes) annually by 2021.[1] Deployments of IoT will mean that Internet connected devices will be found in almost everything that is part of our daily lives — buildings, homes, cities, medicine, food, and even the human body. This level of connectivity will have enormous implications for society, for social institutions and for social norms.

The ability for anyone, anywhere to share content with the rest of the online world is a powerful democratising force. However, it also will present challenges to society. In the future, the community of Internet users will need to take proactive steps to protect itself from threats such as censorship and fake or biased news. Access to sound information may become a luxury, dividing the society along socioeconomic lines. Technological changes, such as AI and automation will change the labour market, displacing some jobs while creating new ones. All this means that it will be critical for society to plan for these disruptions in order to adapt and to mitigate the negative impacts on people and communities.

One thing is certain — in the future, the line between our online and physical lives will blur, if not merge together.

[1] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

The emergence of a global, Internet society

The Internet has always held the promise of expanding access to information and building an open and opportunity-rich society. It empowers individuals to connect, speak, innovate, share, be heard, and organise. In the Internet's earliest days one of its founding fathers, Vint Cerf, believed that a society would emerge from the Internet — an 'Internet society'. At the same time, there is an increasing awareness that the Internet's promise as a force for good may be fundamentally undermined going forward, a result of increasing cyber threats and governments' reactions to those threats, as well as decreasing levels of trust in the Internet.

> "
>
> There is an increase in virtual communities, like religious, art or social, which can be a good thing for the world since it can help bring more openness and for people to know each other and learn to tolerate each other. This will be especially important for Africa.
>
> Technologist, Africa

Overall, respondents feel that there already exists a strong ability to use the Internet to facilitate social change today, which will only get stronger in the future.[2]

There are big forces at work that challenge the promise of the Internet, including:

- The deterioration of online behaviour that undermines collaborative dialogue and deepens polarisation within society
- The impact of automation on work and play
- Divides across society between those who are able to adapt to an ever-changing world and those who are not

Norms of online behaviour

As this global Internet society emerges, we should not be surprised that the problems in society — hate, violence, bigotry — are finding their way online. U.S. Internet experts participating in a 2016 Pew Research Center and Elon University survey predicted that uncivil behaviour will persist online and possibly worsen in the coming years. As Vint Cerf noted, the Internet is like holding up a mirror to society — with all of the good and bad that goes with it.

[2] Future of the Internet Survey 2 - Question 21: "To what extent can individuals use the Internet in [RESPONDENT'S REGION] to facilitate social movements that affect significant change"?

> “
>
> The Internet changed concepts and things that were not acceptable before became acceptable — due the dehumanization. Being rude became easier. It took away the human element of interaction.
>
> Government, Middle East

> “
>
> User behaviour on the Internet, from social media activism to cyberbullying, from crowdsourcing to cyberterrorism, from political mobilization to criminal dark web activities. The Internet is being used for the good, as we originally know, the bad, and now the ugly. Illiberal forces and pressures will increase unless the Internet community itself can demonstrate self-regulation fast enough. The negative forces currently using or abusing the system have demonstrated powerful impact that begs for reaction far more than the positive impact of technological, scientific, humanitarian, social progress wrought by the Internet in its early years.
>
> Technologist, Asia

Anonymity is often cited as an enabler of bad behaviour, allowing users to adopt behaviours they’d never think of using when interacting face-to-face. And yet anonymity also allows people to speak freely without fear of retribution or harassment.

The challenge for the Internet going forward is whether society can harness the power of technology and the ingenuity of the private sector to develop norms of behaviour so that people can interact safely within their networked communities.

While concerns about bullying, hate speech and violent extremism are not new to the Internet, it is only recently that a concerted effort has arisen to see how Internet solutions can be brought to bear to reverse the tide.[3]

> “
>
> There is a tension between an open society and a closed society as espoused by extremists. The Internet is becoming a battleground for the larger societal ideas/tensions. The extremists have an online strategy — this should be paid attention to. There will be question around control and ethos of the Internet. Are there going to be new norms on the Ethos of the Internet and how does the political establishment view this?
>
> Private Sector, Africa.

But these Internet solutions may require tradeoffs for Internet users. Anonymity and free expression may fall by the wayside in the drive to develop technology solutions and social norms to moderate online behaviour.

> “
>
> I think of the old days when the Internet was like a village. We seemed to have ethical guidelines in our email community! We learned what would be considered our ethics. This is missing now that the Internet has been introduced to the general public. People simply enjoy the freedom but with a loss of respect. They leave codes of conduct in the real world when they are in the cyberworld.
>
> Technologist, Asia

[3] http://www.pewinternet.org/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/

Changing nature of work

As automation and Artificial Intelligence fundamentally reshape the nature of work, leisure time and many other aspects of life, the basic fabric of society will be tested. Economic transformation, driven by automation and big data, will generate a host of new challenges around job displacement and economic inequality. Yet, economic transformations at this scale have precedents in history — it is no coincidence that current developments have been popularised with the term "the Fourth Industrial Revolution". And while there is no consensus about how fast the change will come, there is widespread agreement, and even anxiety, that major shifts are on the horizon that will have widespread implications for workers and society.

> "
>
> As more and more jobs are automated, people will push for a guaranteed minimum income. If machines are doing all the work, we still need an income.
>
> Civil Society, North America

Workers, communities and governments are unprepared for how to deal with the society-wide implications of AI and automation. As new jobs appear, the future of some workers will be thrown into doubt as old jobs either evolve or disappear. Management roles and specialist skillsets will not be immune from replacement or augmentation by AI, leaving us with some difficult questions to answer, including 'how do we train the next generation when we don't know which jobs we are training them for'?

As society struggles to absorb and adapt to these changes and their ramifications, new divides will appear between those who are suitably trained for current and future employment and those whose employment is dependent upon sectors that are no longer sustainable.

> "
>
> There will be job destruction (outsourcing, IA, disintermediation) but also the creation of new jobs, including in the "local economy" based on 3D printing, renewable energy (smart grid) and Internet of Things. The big question is how societies will manage to handle the redistribution between the winners and the losers in the transition period. Interesting ideas include the universal allowance granted to all citizens pioneered in countries such as Finland.
>
> Private Sector, Europe.

We cannot predict the final impact of emerging technology, especially on employment, but we do know that the pace of change will continue to accelerate and that many are ill-prepared to deal with the shifts in the short term. Flexibility, adaptability and real-time reskilling across economy and society will be key to thriving in the future. The solutions do not lie in holding back the tides of innovation but rather in preparing now so that society can fully benefit from an AI-enabled future.

Related to: Artificial Intelligence; Personal Freedoms & Rights; The Internet Economy

A changing media landscape

Internet technologies and social media platforms built on new business models will continue to reshape journalism and the media industry, impacting communities, trust in institutions and overall social cohesion.

The growth in citizen journalism, and the use of social media and online video platforms have already redefined the media landscape. Today, anyone can post "news" to these platforms, be they traditional media companies, a teenager in a remote community, or one of the many new online media outlets that have emerged in recent years.

> "
>
> The online version of Gresham's law (bad money chases out good money). In this case, social networks and commentary are increasingly impacted by the loudest voices, that are drowning out the rest. This will significantly influence how websites are designed, comments are mediated, and how the Internet is used in political and social discussions.
>
> Private Sector, Europe

As we move to seamless connectivity across different platforms and networks, users will leverage all manner of devices to share stories whenever and wherever they happen. With new forms of media emerging, more Internet users from all around the world will become de facto journalists, uncovering corruption or disclosing attempts by institutions and governments to limit basic rights. This will be especially important in countries where citizen journalism is an important alternative to government-controlled media.

> "
>
> Question is if it will continue to exist or government will clamp down. One track is that the traditional media will need to adapt to the Internet — "non-traditional self publishing" media in the middle east will continue to grow.
>
> Civil Society, Middle East

However, while the Internet can have a democratising impact on the media, this new environment also gives rise to some unintended consequences. A media landscape based on view-based revenue models will continue to challenge the revenue models of traditional media institutions . The old model of advertising and subscription revenue is being replaced by "clickbaits" and the dissemination of "fake news", a trend that undermines trust in online content. A Stanford University study found that 82 per cent of U.S. middle school students could not tell the difference between a real news story and "sponsored content".[4]

> "
>
> Traditional media is disrupted by the digital age. In-depth reporting is not strong now, and this hurts democracy. Yet the media is a pillar of democracy.
>
> Civil Society, Europe

New media divides will appear between, for example, citizens informed through free or low-cost populist and social media news sites on the one hand, and networks and paywall news on the other. This divide will be exacerbated by populist politicians playing with echo chambers, promoting extremism, and undermining discourse and critical thinking. It will feed conspiracy theories and weaken democracies. Media's role in society as a counterweight to the excesses of power and corruption will be challenged.

> "
>
> Will Internet be used as an information-sharing opportunity, bringing the people closer, OR would it be used a lobbying or media tool to capture people's minds and divert their attentions from serious issues by keeping them busy in "fun"?
>
> Academia, South Asia

Already, media companies and Internet platforms are under pressure to invest in tools to ensure that news remains credible and fact based as well as a positive force for society. Technology, in particular AI, will make news delivery faster and more efficient, with algorithms not only selecting and compiling news stories, but also being used to fact and source-check. AI will also facilitate the generation of stories that are more tailored to algorithmically-determined societal or community sentiment — responding in real-time to catastrophes and other human interest stories. It may bring efficiencies to traditional journalism by freeing up journalists to do more in-depth and nuanced writing.

Related to: The Internet Economy

[4] https://sheg.stanford.edu/upload/V3LessonPlans/Executive%20Summary%2011.21.16.pdf

Governments in search of their roles in the new digital era

In the next five to seven years, governments will be challenged to evolve and adapt to new technological and economic changes and the implications they have for society.

The roles and responsibilities of governments and the private sector will blur as the private sector takes on responsibilities traditionally assumed by governments. For example, the deployment of so-called smart city infrastructure, while offering a wide range of benefits to constituents, will also enable the collection of vast amounts of data, largely by private entities. Citizens and society will need to adapt to the changing role of governments, as the privatisation of public services and public spaces threatens to obscure accountability and responsibility.

> “
>
> I think in the future people will be more dependent on mobile technology and the Internet of Things so governments will seek ways to use this technology to achieve their goals.
>
> Academia, Latin America

> “
> Privatization of Governance — private sector is displacing governments as the local of policymaking (inc. policing/law enforcement, intellegence) — including in the enjoyment of human rights.
>
> Civil Society, North America

Governments will also be pressured to step up in areas traditionally led by the private sector. For instance, some countries may attempt to counterbalance the weight of dominant media platforms, stimulate the emergence of accurate information or limit the influence of fake news on citizens.

As governments use the Internet to deliver more services, the relationship between governments and citizens will become less human. Voting, identification and other services will be automated, resulting in the more efficient delivery of higher-quality services. While this will offer tremendous potential in terms of efficiencies and broadening access to government services, it will also create anxieties in the short term, as the institutions that have governed societies for generations evolve.

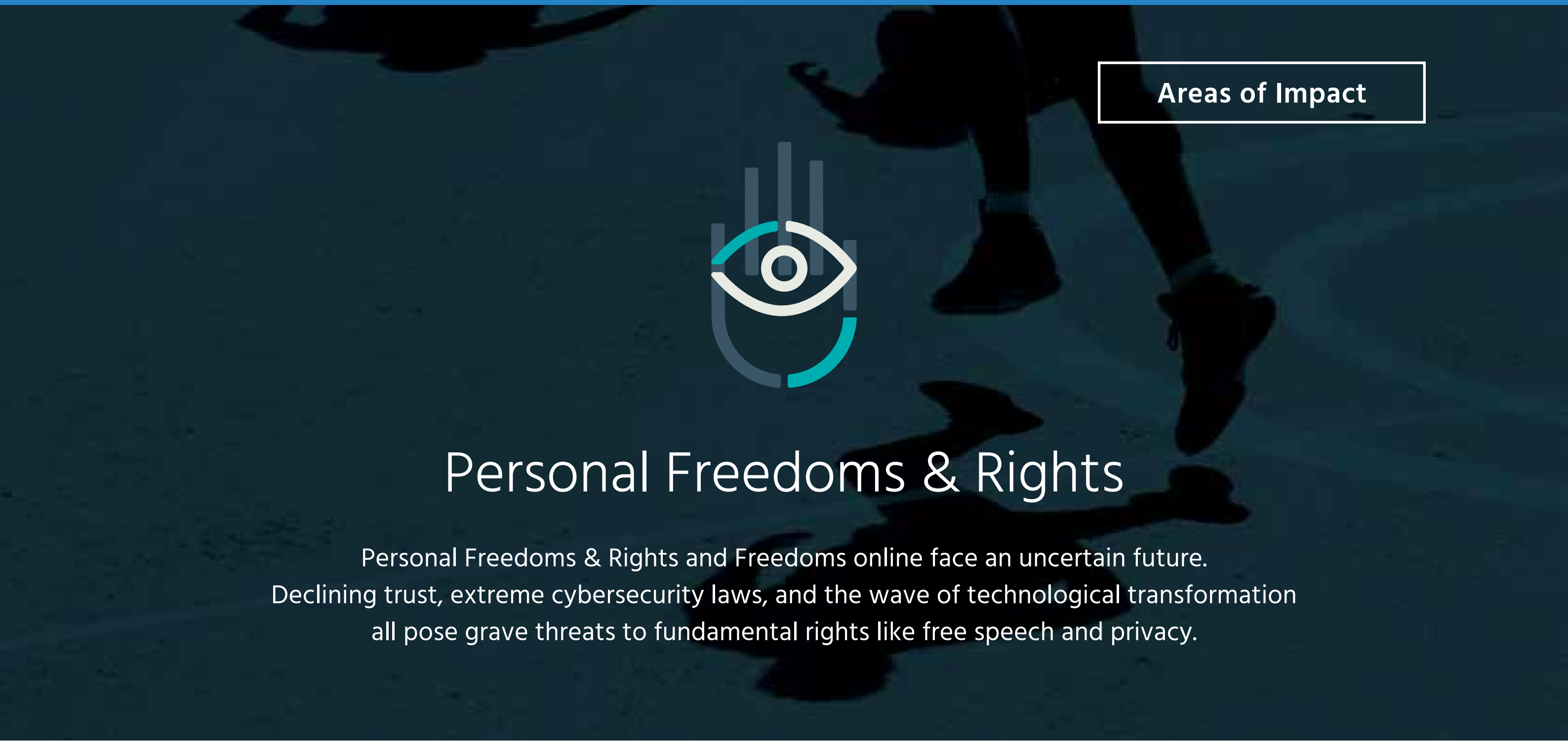
> **Overall, respondents feel that there already exists a strong ability to use the Internet to facilitate social change today, which will only get stronger in the future.[5]**

Finally, as the Internet permeates every aspect of society, politics and the economy, the role of government vis-à-vis the Internet will necessarily shift. Many in our community believe that governments will seek a much stronger role in the development, deployment and use of the Internet and that existing policy tools are ill-suited for the Internet age. Inward focused government policies could stifle cross-border information flows and threaten the global digital economy. Ever stronger claims of cyber sovereignty and protectionist policies will increase risks of technical, policy and commercial fragmentation of the Internet. And a growing number of countries will purposely use the technology to monitor and isolate their people from the rest of the world. This changing role of government will have implications for networked societies around the world that are based not on national borders but on communities of interest that span the globe.

With increasing international data flows, services and goods will come a need to agree on international norms. Some predict that, in the absence of an agreement on universal norms, regional agreements will multiply and accelerate the emergence of a multipolar world organised around new blocs of countries and societies.

Related to: The Internet & the Physical World; The Role of Government

[5] Future of the Internet Survey 2 - Question 21: “To what extent can individuals use the Internet in [RESPONDENT’S REGION] to facilitate social movements that affect significant change”?



Personal Freedoms & Rights

Personal Freedoms & Rights and Freedoms online face an uncertain future. Declining trust, extreme cybersecurity laws, and the wave of technological transformation all pose grave threats to fundamental rights like free speech and privacy.

> **As the scope and severity of cyber threats intensifies, and as global Internet platforms are used to deliberately spread disinformation, users will lose trust in the Internet.**

> **If aligned with human interests, advancements in technology will change the lives of people all across the globe by making the delivery of critical services more efficient and by transforming education, healthcare, and many other aspects of the economy and society.**

> **Advanced deployments of AI & IoT will result in the generation and collection of enormous amounts of information about individuals that can be analysed in ways that are deeply personal and that will raise the potential for a "surveillance society" to emerge.**

> **All governments are under increasing political, economic and social pressure to respond to cyber threats, terrorism and violent behaviour online. Measures that may be intended to secure cyberspace will increasingly undermine Personal Freedoms & Rights.**

Overview

For many, the growth and ubiquity of the Internet is a sign of progress and innovation. They see the Internet as an enabler of human rights such as free expression, free association, and social empowerment. The Internet allows people to create and join new communities and eliminates geographical barriers to making connections. Younger users and those in developing countries are particularly optimistic about the future of the Internet and the ability to use the technology to better their lives and create their futures. And yet, many in our community are worried that the future will see greater challenges to core Internet rights like privacy and free expression.

The future of the Internet is inextricably tied to people's ability to trust it as a means to improve society, empower individuals and enable the enjoyment of human rights and freedoms.

Powerful Internet-enabled data analytics and artificial intelligence will raise important questions about the future of personal autonomy and decision-making and a lack of transparency may undermine user trust. As the scope and severity of cyber threats continues to grow, governments will put stronger measures in place, often in the name of national security, that will impact personal freedom and human rights. We already see a decline in Internet freedom across the globe and we fear that, without a change of course, personal freedoms and rights online may well be nearing a point of irreversible decline.

The Loss of Trust in the Internet

Ultimately, the power of the Internet hinges on users' willingness to trust it. They must trust that their data is secure, that their interactions will be respected, and that their expectations of privacy will be met, among other things. Unfortunately, current trends tell us that trust in the Internet is on the decline, in large measure due to the rising numbers and types of cyber threats and concerns about fake news and disinformation.

The 2017 CIGI/IPSOS study revealed that: "A majority of global citizens are more concerned about their online privacy compared to a year ago".[1] People in the developed economies said they were losing their trust in the Internet because they are worried about "government behaviours and control by corporate elites". Similarly, respondents to a recent Internet Society survey in Asia Pacific listed cybersecurity, data protection and privacy among the top five Internet policy concerns for the region[2]. And there are broader implications for development, with one member of our community suggesting that "access will not be achieved as hoped if trust is not addressed". Having said all this, Internet usage in general continues to rise, social media remains popular, and the sharing economy shows no signs of slowing down.

> "
>
> Lacking progress, the Internet risks losing "simple", "honest" people to trolls, spammers and malware. Commerce could collapse on the internet due to a lack of trust and effective legal recourse.
>
> Technologist, Europe

[1] https://www.cigionline.org/internet-survey
[2] https://www.internetsociety.org/news/cyber-security-tops-list-concerns-internet-users-asia-pacific

Internet users fear that they will be on their own when it comes to managing their online security and the never-ending parade of data breach announcements by industry and government alike is evidence of the challenge. News of cyberattacks, identify theft, and the hacking of corporate and government systems make users feel increasingly powerless to protect themselves or their data. When there is a data breach, the user often suffers most, though with little recourse.

With greater amounts of data being collected about many more aspects of our lives, we will have even more to lose in future data breaches. If the burden of risk is not more widely shared — through clearer legal accountability and greater investments in security — the decline in overall trust will accelerate.

> “
>
> A lack of trust on the Internet could lead to regression.
>
> Technologist, Africa

> “
>
> I think that trust has a very serious impact of future adoption and development of the Internet. With more data floating around, data protection and personal information security is another uncertainty that I can think of.
>
> Private Sector, Asia-Pacific

The lack of clear security *and* privacy standards for the Internet of Things raises the prospect of a “digital environmental disaster[3]” — a scenario in which abuse of connected objects by criminals, terrorists or even governments escalates to the point that the IoT environment becomes a polluted space in the eyes of consumers. A 2016 Accenture study of consumers in 28 countries concluded that “consumer technology industry does not have the fundamentals in place—and the consumer trust established—to push into more personalised and sensitive areas as it searches for the next wave of innovation”[4]. This same study noted that a lack of trust is already impacting the market for IoT as consumers remain cautious about whether or not the devices and their data will be secured.

Some, including Internet security expert Bruce Schneier, have gone so far as to suggest that, absent clear moral, ethical and political decisions, there might be a flight from connectivity as people reconsider how much should really be connected[5].

> “
>
> Security concerns may start to prevent users from going online, and once online may impact their usage, particularly with relation to sensitive political and personal issues”
>
> Civil Society, Europe

[3] https://otalliance.org/system/files/files/initiative/documents/iot_sharedrolesv1.pdf
[4] https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf#zoom=50
[5] http://www.elon.edu/e-web/imagining/surveys/2016_survey/internet_of_things_infrastructure.xhtml

Government actions also undermine user trust in the Internet around the world. Revelations about surveillance and emerging details about cyberattacks leave end-users wondering if they will be collateral damage in a conflict they are barely aware of and have little control over. Many politicians are framing security in ways that suggest a trade-off is needed between rights and freedoms on the one hand and security on the other. This caused one member of our community to suggest that "the Internet is not leading to a rights-based society but rather to a surveillance society".

> "
>
> Not meaning to sound gloomy, but all these shutdowns, filtering, and wide-scale surveillance have existing and potential users feeling like the Internet has become a massive platform for replicating offline oppression in the online world.
>
> Technologist, Caribbean

There is no single answer to the trust dilemma, but many current activities will help to improve the future Internet security environment for end-users. Stakeholders are devoting even greater resources to security, with one estimate suggesting global spending on cybersecurity may exceed $1 trillion between 2017 and 2021.[6] More messaging apps are using end-to-end encryption. Greater deployment has increased the volume of encrypted web traffic. IoT security frameworks are being developed. Internet companies are also taking steps to address concerns about fake news and violent online content. And, finally, serious global and regional efforts[7] to promote policy collaboration among stakeholders, including governments, are beginning to show results.

> "
>
> Is enough work being done on enhancing the web, making it more distributed, and more secure? Are we looking at new technologies for example how the bits we download each second can come from different sources to make it more difficult for people to know what you are doing online? I can imagine that this will happen one day soon and will have a great impact on the internet, and will make users more comfortable and trusting of the internet.
>
> Technologist, Middle East

> **Respondents already believe that the general public exhibits a degree of trust in the Internet today and predict that the general public will exhibit a higher degree of trust in the Internet (and low level of concern for most uses) in the future.[8]**

Related to: Cyber Threats

[6] Cybersecurity Ventures' "Q2 2017 Cybersecurity Market Report": https://cybersecurityventures.com/cybersecurity-market-report

[7] For example: 2016 OECD Security Guidelines; 2017 African Union / Internet Society Internet Infrastructure Security Guidelines for Africa; Global Commission on Internet Governance; Global Commission on Cyber Stability.

[8] Future of the Internet Survey 2 - Question 32: "To what extent does the general public trust the Internet and its integration into daily life"?

AI and IoT will simultaneously empower and weaken users

Emerging technologies such as IoT and AI hold the potential to make the delivery of critical services more efficient and drive advancements in education, healthcare, agriculture and many other aspects of the economy and society. Armed with better information, citizens will be empowered to make more informed decisions and to hold governments and businesses accountable.

> “
>
> More sharing equals less privacy; people continue to trade convenience for security.
>
> Technologist, North America

As one technical expert in Europe suggested, “AI has the opportunity to increase transparency by making it easier to actually answer the question of where information is stored. So, in the future we can use our phone, our iPad, bracelet, computer, whatever kind of device we have, and ask where that specific company stores data about us and make the company accountable”. Individuals may be able to develop their own algorithms in order to track how they are being tracked. This scenario, one in which dramatic advances in Artificial Intelligence deliver results that have a positive impact on people’s lives, is only possible if humans remain in control of the technology and guide its development and deployment in ways that are consistent with human values.

There is another possible future in which AI and similar technologies are designed and deployed so fast, and with profound social impact, that the ethical and moral frameworks cannot keep up. In this scenario, advancements in AI and IoT may threaten human rights and personal freedoms and have huge implications for the transparency of decision-making and expectations of privacy. Algorithms use enormous quantities of information, much of it collected in ways that are not transparent to individuals. How will we ensure accountability when algorithms make decisions that affect people’s lives but are difficult to understand or to appeal?

> “
>
> Data collection is now a big privacy concern, especially when individuals are being observed by connected devices.
>
> Government, Africa

> “
>
> In the case of Big data and IoT who is responsible and accountable? We don’t know who to blame in case of abuse of a product or service: the designer, the manufacturer, the owner? How to include human right aspects into these artificial intelligent and IoT objects is a key question.
>
> Private Sector, Middle East

Some users already worry about the vast amounts of their personal data being collected and feel powerless to protect their personal privacy. Already, systems use data profiling to draw inferences about individual beliefs, preferences or habits in ways that are deeply personal.

> People are worried — they don't know how much algorithms affect rights and data of persons.
>
> Civil Society, Middle East

With advances in AI, the collection of personal data will go beyond questions of privacy to a potential threat to personal autonomy. In a world where a lifetime of personal data-collection begins even before birth, and where that data is used to make decisions that deeply impact people's lives, people worry that they will lose the ability to question decisions and determine their own futures.

> The rise of data-driven services leads some to worry of a Minority Report-style future in which our course in life is mapped out for us, eroding our ability to make free choices. Then there's the worry that the data savvy might become a web-empowered elite, keen to keep those who are not digitally enabled firmly on the lower rungs of society.
>
> Private sector, Europe

Important work to ensure that human values drive technological and business advances is being done in the research, industry and policy communities. Whether the future Internet sustains our freedoms and rights, or whether it pushes them past the point of no return, will depend on whether this work can keep pace with the deployment of technology and has the continued buy-in and commitment of all stakeholders.

Related to: Artificial Intelligence; The Internet & the Physical World

Freedoms in light of the growing role of governments online

From its early days as an information-sharing network, the Internet empowered users and communities and enabled more transparent and accountable governance, raising awareness of human rights violations and gathering evidence for prosecution. Yet, as the scope and severity of cyber threats continues to grow, governments will put stronger systems in place, often in the name of national security, that will impact personal freedom and human rights. In some parts of the world, the Internet is being used as a tool for pervasive data collection, surveillance and control. This is reflected in an overall a deterioration in Internet freedom across the globe and we fear that, without a change of course, Personal Freedoms and Rights online may well be nearing a point of irreversible decline.

> “
>
> Liberal values are weakening around the world [which] doesn’t bode well for the Internet. Winter is coming.
>
> Civil society, North America.

Freedom House, a non-governmental organisation active in Internet policy, has documented a decline in Internet Freedom for the past six years[9]. Many of the Internet Society’s global community echo this sense of a decline in rights and freedoms — for them, restrictions such as Internet shutdowns are a consistent threat to their livelihoods, communities and future opportunities.

“keep it on” principles[10]

The very tools that facilitate human empowerment can also be used to constrain it, and as the Internet becomes part of everything we do, the temptation for governments to use it to constrain will only grow.

As many governments are pressured to respond to cyber threats, online hate and terrorism, even rights-respecting governments may see a false choice between security and human rights. For example, efforts to undermine encryption or ban anonymising tools like Tor for national security purposes threaten free expression and privacy of individuals everywhere. While new technologies can offer the promise of more efficiency and new services, they can also be used by governments — in the name of security –to create a surveillance society, undermining freedoms and privacy.

> “
>
> One of the biggest surprises is that democratic countries are seemingly starting to give up their leading role for an open Internet that supports online freedoms, in the wake of new national security threats and surveillance apparatus
>
> Civil Society, Europe

Although there is a collective responsibility to ensure that the Internet is not used as a tool of control, much of the burden will fall on the shoulders of the companies running networks or platforms and manufacturing connected devices. How industry and particularly the Internet companies react to government pressure will help determine the future of the Internet as a space for free expression or for censorship and surveillance.

[9] https://freedomhouse.org/report/freedom-net/freedom-net-2016

[10] https://www.internetsociety.org/african-youth-why-internet-matters

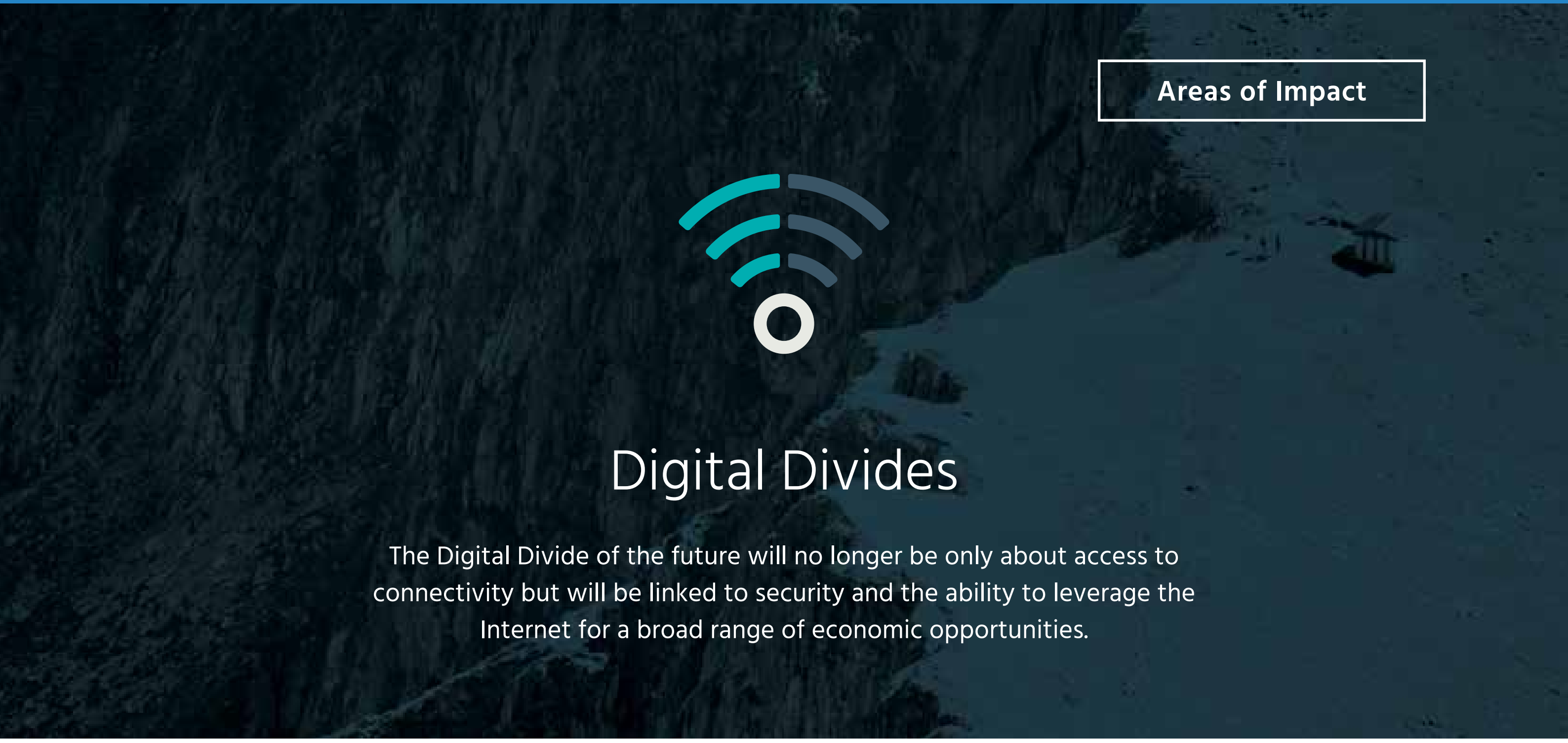
> “
>
> It was thought that the Internet could bring democracy to all countries if they were connected to Internet but we learned that is not the case. The impact of Internet on politics is not as big as thought. Because of censorship there is a violation of human rights. China and Russia are protecting the stability of their countries. Western countries do not see it this way. This will be a big issue in the next 5–7 years.
>
> Government, Asia-Pacific

Stakeholders in our community still see the Internet’s underlying values of openness and global reach as fundamental and worth protecting. Indeed, it is clear that the core values of the Internet are not tied to any one geopolitical ideology — they are seen as universal.

> “
>
> The Internet will be increasingly used for education, to make economic transactions, to make political decisions and to defend our rights. Attacks on privacy will become more apparent. Citizens will be more aware of the risks and threats that exist on the Internet.
>
> Civil Society, Latin America & Caribbean

At the same, these values of openness and global reach will become more tenuous and cannot be taken for granted. All stakeholders will need to be vigilant and persistent if we are to maintain these core values in the face of the increasing claims of national security and public order. New and emerging technologies may well be part of the solution: rather than using them to undermine freedoms and rights we should use them to bolster the Internet’s core values of openness and global reach and counter the global trend of weakening freedoms and human rights.

Related to: The Role of Government; Cyber Threats



Digital Divides

The Digital Divide of the future will no longer be only about access to connectivity but will be linked to security and the ability to leverage the Internet for a broad range of economic opportunities.

> **As new threat vectors emerge, a security divide will materialise between those with the knowledge and resources to protect themselves from cyber threats and those without.**

> **Consolidation of networks and platforms within a few organisations will affect the ability of networks to grow and scale and will limit the ability for new players to emerge.**

> **The adoption of Artificial Intelligence and the Internet of Things will transform the global economy offering opportunities for the developing world; however, without adequate infrastructure and broader economic opportunity, many nations may be left behind.**

Overview

While we still have a long way to go, data shows that the digital divide as we have historically defined it — those that have access to the Internet versus those that do not — is closing. From small community networks in some of the most isolated parts of the world to large-scale infrastructure development projects, we are making progress toward connecting the 53 per cent of the globe's citizens who are not yet online.

However, new divides will emerge in the future driven by developments in technologies and networks, as well as by the lack of economic opportunity and cyber readiness. Disparities in infrastructure development, high costs of connectivity, restrictions on access, barriers to entrepreneurship, and lack of skills and resources will amplify these new divides, hampering the ability of many people to fully enjoy the economic and social benefits the Internet offers, and making some nations even more vulnerable to cyber threats.

These new divides will deepen disparities between countries — in particular, between developing and developed nations — but also within countries. As the Internet transforms every sector of the global economy, the digital divides of the future won't just be about access to the Internet, but about the gap between the economic opportunities available to some and not to others. From the ability to access and share online content to the ability to benefit from the Internet of opportunity, existing inequities between the "haves" and the "have nots" could be exacerbated as technology changes move faster and faster.

The impending security divide

Meaningful use of the Internet depends not only on access to connectivity and the ability to fully benefit from it, but also on the ability to safely use Internet technologies and services. In the future, the skills to understand online threats, and the financial resources to protect oneself from those threats, will be crucial to an individual's wellbeing. As cyber threats mount across the world and individual safety is at stake, we foresee a divide emerging between those who have the knowledge and resources to protect themselves and those who do not.

Security literacy and resources to pay for access to security and privacy protection tools will be essential. Above all, a substantial commitment from all stakeholders to address cybersecurity challenges head on will be critical. Some users, organisations and countries will be in a better economic position to protect themselves online, while others will become more vulnerable. Countries with cybersecurity strategies, the ability to protect critical infrastructure, and the capacity to prosecute cybercrimes will have greater economic advantages than those that do not.

> “
>
> Better and better trust and security issues will allow more and more benefits to the as yet unconnected. Countries with poor credit rating and with poor identify verification will continue to cost their consumers and producers higher risk premiums. This is an area that Government's can help by reducing the transaction costs of doing business over the Internet.
>
> Civil Society. Asia

Vulnerable populations will also be at risk. Individuals and groups like the elderly or poor that are vulnerable to crime in the physical world are especially vulnerable to cybercrime. They may lack the skills to protect themselves and are more likely to be targets of fraud, scams and theft.

> “
>
> The Internet will create a new social class rising above the others. Women will have more opportunities with increased virtual mobility. An area that will challenging then is online safety and privacy.
>
> Technologist, South Asia

Developing nations struggling to get online and those that are lacking in cyber readiness will be disproportionately affected by cyber threats . As U.S. researcher Gamreklidze argued in 2014, “Cyber security is the area where both of the problems typical to developing countries, of the access to ICT and the skills necessary to use them, overlap”.[1] This knowledge and resource gap will only widen existing economic and security divides.

> “
>
> But inclusion also means literacy. We know how to teach and learn the alphabet but we still don’t know how to do that with the Internet.
>
> Government, Europe

While new Internet-based technologies like the Internet of Things promises economic and social opportunity, their deployment is introducing cybersecurity challenges across all sectors of the economy. Because the ICT sector is no longer isolated, threats to the communications infrastructure are now threats to the entire economy. Developing countries that are already behind when it comes to cybersecurity readiness will find themselves struggling to keep up with the pace of changing security threats.

> **While our community believes that policy makers will become better at keeping up with Internet technology, they are uncertain as to whether the pace of change and innovation will surpasse the ability of policymakers to keep up.[2]**

> “
>
> We talk of e-government but this can not happen if the Internet cannot be trusted.
>
> Technologist, Africa

At the same time, new threat vectors will multiply as more and more aspects of our social and economic lives move online. The ability of governments to secure their domestic infrastructure — ranging from power plants and hospitals to communications networks — will be critically important because insecure networks put social services at risk, from police and emergency services to water treatment facilities and financial services. In essence, those on the disadvantaged side of the digital divide will become easy targets for bad actors.

Related to: Cyber Threats; The Internet & the Physical World

[1] Cyber security in developing countries, a digital divide issue http://www.tandfonline.com/doi/abs/10.1080/13216597.2014.954593

[2] Future of the Internet Survey 2 - Question 28: “How well are policymakers able to keep up with the pace of change in Internet technology, use, and business”?

The new digital economy — providing opportunities or deepening divides

The future digital economy promises tremendous change at a pace difficult to fully grasp. Deployments of Artificial Intelligence, for example, will transform economies in ways we are only beginning to imagine. The key to success in this fast-paced environment will be adaptability. Countries, businesses and even workers must be agile and have the capacity to learn quickly in order to thrive in the Internet economy of the future. In a global economy characterised by rapid change, the digital divide will evolve and possibly deepen based on the ability to simply keep up with technology.

> “
>
> E-Commerce will continue to blossom and have a greater share of the global economy with governments putting more emphasis on infrastructure and technological facilities to expedite the transformation from an offline to an online economy. Countries not well equipped to deal with this may be left lagging in terms of economic progress.
>
> Civil Society, Europe

Digital Divides

Those regions of the world that are already struggling with basic Internet access will be left further behind in the global economy of the future. As technology accelerates, some wonder if a permanent underclass will emerge. We may also see divides emerge between those communities, businesses and economies that can absorb change and those who cannot. Indeed, if all communities and countries do not have the resources and/or capacity to plan for and adapt to this economic transformation, the existing economic divide will only be more pronounced.

> “
> Providing connectivity to marginalized populations does not necessarily open the world in these impoverished areas. Connectivity and social networks are instruments that, many times, replicate poverty. The problem is not having a strategy behind providing connectivity.
>
> Internet Society Chapter, Latin America

> “
> We may be seeing increased pressure from industries not ready for the Internet revolution that may result in short term protective regulations that will hinder Internet development and benefits.
>
> Technologist, Africa

Despite the fact that they could benefit the most from IoT[3], developing nations in particular may be left behind they lack both the connectivity infrastructure as well as the policy frameworks to leverage the wave of innovation. As Michael Wolf wrote in Forbes in 2015, “While there will be no doubt be some big winners in all the various IoT markets . . . the reality is that like any big tech category the majority of the spoils often go to a very few”.

> “
> [There is] A broadening gap between the golden billion and the rest of the humankind in terms of access to and benefits from all the pluses of the ICT and Internet development.
>
> Technologist, Asia

While we are making progress toward closing the digital divide, gaps between the connected and unconnected will persist. Many countries currently rely on mobile phones for affordable access. Without investments in core infrastructure to support the growth in connected devices, citizens will be unable to benefit fully from the digital economy. IoT and other new technologies require access to bandwidth; investments in infrastructure, such as reliable power supply and data centres, are critical to ensure that these services are reliable. As one participant from Guatemala noted, “IoT will place a greater load on already taxed bandwidth. Higher bandwidth technologies must be developed and deployed”.

[3] https://arc.applause.com/2015/12/02/internet-of-things-growth-developing-countries/

Digital Divides

> In the coming years, the deployment of fibre optics especially national backbones will cover between 70–80% of respective countries in the Africa region.
>
> Technologist, Africa

> The "digital divide" will be characterised by the level of access to electricity.
>
> Academia, Africa

Clearly, the future digital economy offers opportunities for emerging markets well beyond the ICT sector itself — the Internet of Things is driving innovations in clean water, disaster preparedness and relief, healthcare delivery and disease prevention. While some worry that market consolidation will deter entrepreneurship, we believe that the spirit of creativity is still thriving. The Internet, based on open standards and permissionless innovation, democratises entrepreneurship and the new innovations are surfacing outside the traditional geographic clusters like Silicon Valley. As two South African entrepreneurs observed: "Firstly, technology innovation is going to give us the data we so desperately need to understand how to solve the problems we face, and, secondly, will drive the cost-to-serve down to a point where we can address the problems effectively at the required scale".

Our community is optimistic about bridging the future digital divide. In fact, all stakeholder groups and regions feel that the gap between regions in their ability to benefit from and participate in the Internet will decrease in the future.[4]

> There is so much money in the wireless delivery market (low earth satellites, Google loon, FB, etc) that it seems like something will click and we'll finally solve the access issue.
>
> Government, North America.

The ability of new players to emerge could be limited if the trend toward the consolidation of networks under the control of a few large, global players continues. Large Internet platforms are deepening their market positions, dominating Internet infrastructure, services and applications. Smaller networks will simply be unable to compete with large, global companies that are able to offer services cheaper and make investments into the development of new products and infrastructure development.

> In developing countries from Latin America and Africa, we have more consumers than producers, so we need to have a more balanced field in order to have everyone enjoying the economic benefits of the network.
>
> Technologist, Latin America.

Our Caribbean Islands and Northern Africa communities predicted a low level of content creation from their region in the future.[5]

If we do not act now to ensure *all* parts of society are ready, able and prepared to harness the power of technology to better their lives, the digital divide will only contribute to deepening socioeconomic divisions.

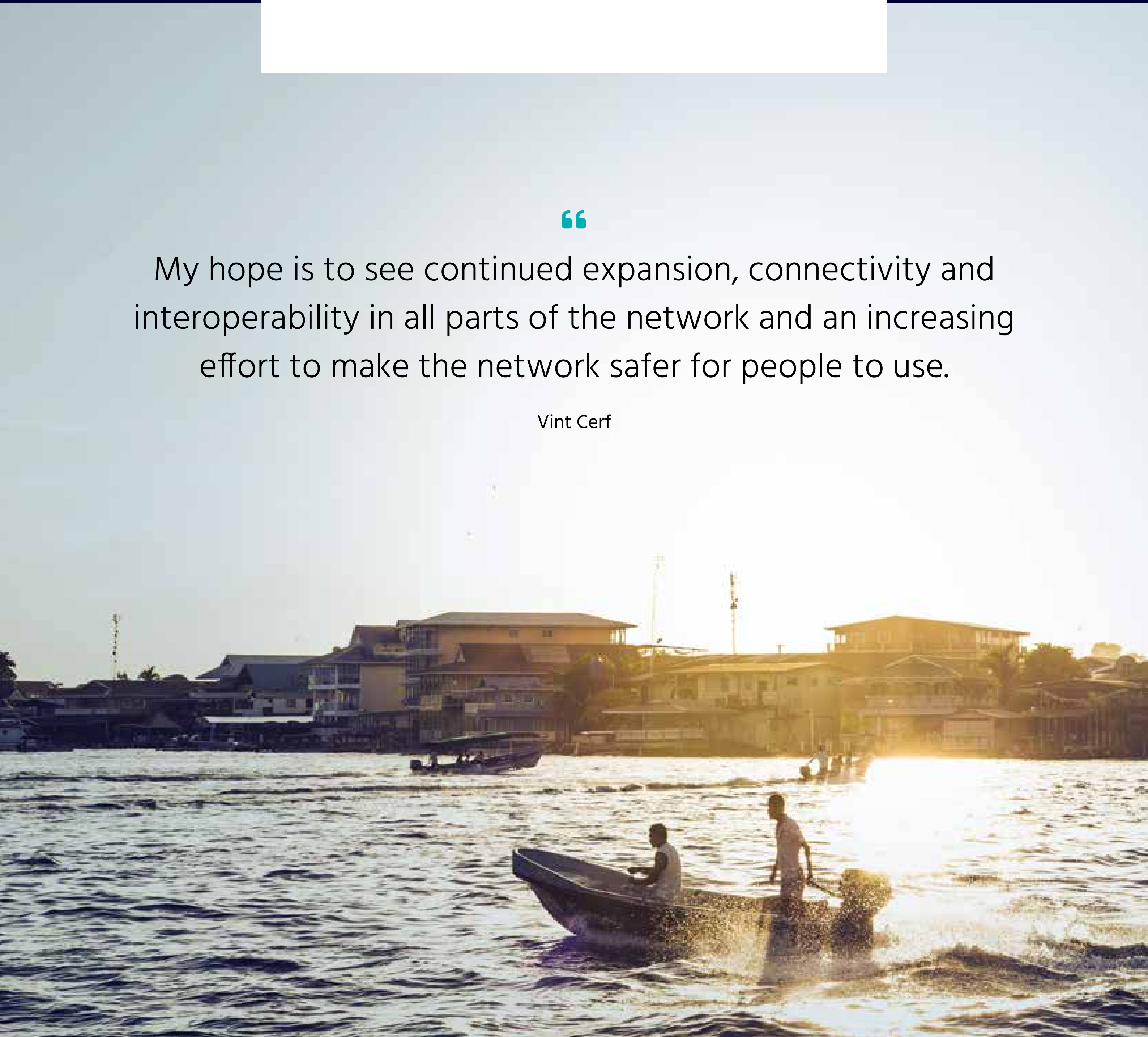
Related to: Artificial Intelligence; The Internet Economy; The Internet & the Physical World

[4] Future of the Internet Survey 2 - Question 12: "How large is the gap in the ability of individuals in different regions of the world to meaningfully benefit from and participate in the Internet"?

[5] Future of the Internet Survey 2 - Question 16: "To what extent do users and companies in [RESPONDENT'S REGION] develop Internet content and services compared to consuming existing content and services"?

8

What if?



> My hope is to see continued expansion, connectivity and interoperability in all parts of the network and an increasing effort to make the network safer for people to use.
>
> Vint Cerf

What if …
government responses to Internet challenges undermine people's fundamental rights?

Shutting down the Internet Shutdowns — How to Crowdsource Your Way Out

Internet shutdowns by governments have become routine. Got an election coming? Shut down the network to stop people organising. Annoyed by minorities demanding language or education rights? Shut down their region and arrest anyone who complains. Worried that students may cheat on exams? Shut down the mobile network so they can't "phone a friend".

But it turns out that many countries have large diasporas; nationals who moved abroad to work. These people earn good money and like to keep in touch with home. What do they hate most? Internet shutdowns.

So when the government of Edonnia leaned on telecoms providers to cut off the Internet before a recent election, the two-million Edonnians working overseas swung into action. Crowdfunding via social networks abroad, Edonnian migrants pooled their wages to buy satellite time for friends and family back home.

Back in Edonnia, heads of families asked younger relatives to unlock or "jail-brake" everyone's phones so they could be used on any network. Community broadband groups coalesced with social and religious gatherings to spread know-how and local-connectivity resilience. When the inevitable shutdown began, people hooked up to satellite through hundreds of local nodes, with the main costs covered by family and friends abroad.

Back online, the people condemned the attempted shutdown, and warned the government; "If you want the remittances to keep coming from abroad, keep the Internet switched on". Within hours, the shutdown ended with the government claiming a "technical issue" had been responsible. But the message is clear. Now, not just the technology, but also the people will route around network failures.

Related to: Cyber Threats; The Internet Economy

What if … the rise of new state and corporate powers fundamentally changes our current model of Internet governance?

Angerland Sells UN Security Council Seat to Majuscule

In a closely guarded deal, the Republic of Angerland has effectively sold its rotating UN Security Council seat to the global information giant, Majuscule. Although no official statement has been made, Angerland's Permanent Representation to the UN is now headed by Ralph White, Majuscule's President of Stakeholder Relations. Angerland's next turn as President of the Security Council comes in Spring, 2026.

Majuscule told our New York reporter that White is "on secondment" to Angerland's mission to "share information and ideas". But we have learned that four Department of Foreign Affairs employees, including the UN Ambassador, have been ordered back to the capital with barely time to clear their desks. The delegation has been replaced with Majuscule employees carrying business cards showing Angerland's national symbol, inside the Majuscule logo.

The Security Council president has powers to set the agenda, chair discussions and oversee any security crisis that occurs during their tenure. Respected as an effective and even-handed operator with little skin in the game, Angerland's previous presidencies of the EU and UN Security Council have been very successful. An unnamed but senior UN figure told us; "When Angerland chairs, business just gets done. The Angerlands rarely care about the content, just about getting a deal everyone can live with. But this level of pragmatism is just … I don't know what to say. They literally put a dollar amount on their sovereignty".

In a quid pro quo, Majuscule will extend its Income Boost scheme to cover 25% of Angerland's unemployed, at $8 billion per year for the next ten years. It is worth noting that the Income Boost scheme also provides the company with unlimited access to the participants' data. As a country that relied on technology giants to fuel its boom and now has 40% unemployment, it is perhaps no surprise that Angerland is selling off its few remaining assets and the technology giants are happy to oblige.

Related to: The Internet Economy

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if …
automation and AI create short-term savings for industries but damage their long-term sustainability?

Shortage of mid-career lawyers hits legal profession hard

In 2017, experts had predicted a "decade of disruption". For once, they were right, especially about the legal professions. After the 2008 global financial crisis, law firm fees were too high, even for corporate clients. Traditionally, law firms used just-qualified lawyers for routine legal tasks. The juniors would learn their trade, doing repetitive but essential work, and develop the judgement and experience to move up the ladder.

But in the mid 2010s, law firms essentially stopped hiring junior lawyers. Instead, they invested in AI for routine work like checking land registry records or due diligence. Tasks that took humans weeks could now be done in just a few hours. A recent report estimates that up to 500,000 legal jobs were lost around the world from 2015–2022.

With lower costs, law firm partners who made perhaps $1 million USD a year in 2015 now make an average $5 million each. In a "winner takes all" legal economy, the losers never even started their careers, but the winners did extremely well.

But today, the legal profession faces a global shortage of mid-career lawyers. Law graduates who would have taken junior jobs a decade ago should now be moving towards the partnership track. But with few junior legal jobs then available, most legal graduates left the law or took part-time or short-term jobs. Law firms now face a hiring crisis in the middle ranks. They must pay top dollar to an ever-smaller pool of experienced lawyers, sometimes offering larger salaries than the partners pay themselves.

Law firms now scramble to find experienced lawyers for work that needs a human touch; advocacy, litigation, arbitration, or just applying hard-earned experience and judgement to making deals. For the first time in history, we need more lawyers than we have.

Related to: The Internet Economy

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if …
there was a digital assistant that only had the user's best interests at heart?

Falling for Mishee™

Mishee: is she a neutral intermediary, a digital agent or perhaps even a guardian angel?

I put these questions to Mishee's creator, Imani Armah, the Ghanaian technologist and entrepreneur. We met for an early coffee on the roof terrace of Vida e Caffè in Labone.

"I think of Mishee as a best friend, or perhaps your wiser twin", Imani says with a slightly wistful smile. "Mishee knows your weaknesses, but she doesn't play on them. She asks you simply how much you want to share …"

"Or how little", I interject.

Mishee forces the platforms to negotiate for our personal data, and for many users, that means blocking its transfer.

"There is no one-size-fits-all", Imani says patiently. "Some people like to share more. And we change as we move through life. Mishee makes the platforms listen".

"She empowers users", I say.

"Traditional digital assistants work to keep you in their ecosystem and buy things. Many of my friends resented their devices and distrusted the platforms", Imani says. "We had lost the feeling of happiness you get when technology just works. Mishee is a voice-operated interface for everything, from your TV to social media. She talks to you like she's human, and, most importantly, she's on your side. Mishee gives us the promised smoothness of technology, without the hard-sell".

"You sound almost evangelical", I tell Imani. "How did you manage to invent something the whole world needed"?

"That's easy", she smiles. "People of the global north had fallen out of love with the Internet. But we in Ghana still held its joy and its possibility. In the Ga language, 'mishee' means happiness, or even delight. I created Mishee to share our feeling of delight with the Internet, and I think she has".

Without thinking, I lean across the table towards Imani.

"I think I am a little bit in love with Mishee".

Imani sits back, her hands demurely in her lap.

"You are not the first to feel this way", she laughs, but kindly. "No one liked Big Brother. But Big Sister? We have a different kind of feeling for her".

Related to: The Internet Economy; Personal Freedoms & Rights

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if …
businesses become so reliant on the mega platforms that they lose their independence?

“Global Marketplace”, the View from Eurasia

I started my business in 2022. I’d yearned to be my own boss, and when I had my second child, it was not economic to return to work. I saw a gap in the market for modest but flattering and stylish women’s swimwear. With a loan from my mother’s family, I employed three women in my garage, and more who did piece work at home. We sold through a shopfront on Global Marketplace (GoMo). Within six months, I had more orders than we could fulfil.

I needed to expand so I went to the bank with my order book and accounts. They demanded my husband’s accounts and a guarantee on our home. They kept asking for more information, more guarantees. In the end, they refused me anyway! I was despairing. Then an email popped into my in-box. It was from GoMo.

They’d noticed I had a “significant fulfilment opportunity”, and offered a line of credit and working capital at a low rate. They hold my order book and know all my suppliers, who are also with them. I use their Budget-Buddy service to pay my staff. I even buy much of my personal groceries from GoMo. They know my finances and the content of my professional database better than I do! So of course I said yes. Now I employ thirty women. We sell our swimsuits across the region and meet a growing demand for modest swimwear that isn’t available anywhere else.

But … while GoMo allowed me to fulfil my dream I feel it is now running my business. It keeps pushing faster expansion than I want, and mysteriously favours some retailers and suppliers over others. I don’t have a good feeling about that. Next time it could be me they don’t push, and I have then what would I do? Would they even listen to me?

I have the know-how and I take the financial risk. But while I’m transparent to GoMo, they are opaque me. They hold all the cards. I’m grateful for everything they’ve done, but I feel like an employee again. Except this time, I can’t change platforms as easily as I could change my job. Life is good now, but who knows what’s around the corner?

Related to: Digital Divides

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if …
revenue-starved public services are taken over by the mega platforms?

The quantified welfare recipient; How Majuscule is nudging the unemployed towards independence

“I’m a Majuscule person”, Nick says, referring to the global information company and speaking quickly as he twists the wearable on his ring finger. “Sorry, Nudge. I’m a Nudge person”.

I ask Nick what it means to him to be part of Nudge, a Majuscule-owned and operated program, and the biggest experiment in behaviour modification ever created.

“I’m a better version of myself every day”, he says. “The best person I’ve got it in me to be. Can we walk and talk? I need to hit my steps by noon”.

“Sure”, I say. “How are your targets going”?

“Terrific”, Nick says. “I keep hitting my targets and they keep setting them higher. There literally is no limit to what I can achieve”.

Nick is one of half-a-million people trialling a partnership between Majuscule and the Department of Public Health. Now that so many jobs have disappeared and government welfare provision for the under age thirty is gone, Majuscule provides Income Boost (IB) to the un- and underemployed. IB provides a basic minimum income, training and the promise of eventual employment; the program gives Majuscule control of their personal data, now and in the future. In the Nudge program IB recipients are tracked 24/7 with wearables monitoring their health. If they miss targets, they lose income. They must buy Majuscule -approved healthcare products and services. Many IB recipients are participating in numerous such Majuscule programs, removing the burden of welfare provision from the state.

Nick’s daily targets include walking 20,000 steps, and fifteen minutes each of high-intensity aerobic exercise and mindful gratitude. He must initiate two meaningful conversations per day, with bonus calories awarded for talking to new people, and promote the benefits of Nudge and Majuscule products and services.

The unemployed can become depressed and overweight from lack of stimulation and exercise, but isn’t this invasive?

“Before”, Nick says, “I just couchsurfed and played games online. Went to the food bank or to protests. Now, someone cares what I do and holds me accountable. I don’t have a job yet, but I’m getting closer. I’ve got to stay grateful and positive. I’ll get there”.

Related to: The Role of Government; Media & Society; Personal Freedoms & Rights

What if …
the world actually cooperated to detect and patch zero-day vulnerabilities — and made us all safer in the process?

Saving the World One Zero-day Vulnerability at a Time

2019 and 2020 were bruising years — damaging and destabilising cyberattacks, many exploiting zero-day vulnerabilities, became the norm. Despite endless multilateral meetings designed to build confidence, states were no closer to agreeing norms of behaviour regarding the reporting, stockpiling or use of zero-day flaws. For all the talk, the result was simply a vicious circle: mistrust, leading to more finger pointing; bad outcomes for end users, leading to increased mistrust, and so on.

The key to de-escalation came from an unlikely quarter. In February 2021, an unidentified group created a highly-distributed mesh of cryptographically secured repositories, collectively called BlackBox. They uploaded hundreds of .txt files describing zero-day vulnerabilities. They emailed the CTOs or CIOs of the software and hardware companies concerned — with credentials to access one specific vulnerability — as an indication of BlackBox's credibility. The only catch: each company would only get more information as it demonstrated further action in good faith. Disclose your tally of known, unfixed flaws, and you'd get the tally of how many BlackBox had; publish one patch, and you'd get a key to the next one; upload one of your own unfixed flaws, and you'd get a two-for-one deal, and so on. BlackBox's rationale was that bug bounties alone had never been enough to make the ecosystem healthier as a whole.

At first, few responded, presuming either a phishing scam, or a precursor to blackmail. But no ransom demand arrived, and slowly, incrementally, back channels between researchers who'd done graduate work together built trust in the bona fides of the operation. Word also spread through the tight-knit state security community, who saw — among the published fixes and patches — both zero-days that they had thought only they knew about, and zero-days they hadn't even found themselves. Soon, those in the loop, including major global businesses and state agencies, weren't just pulling down information about their own vulnerabilities, but offering up information as well.

Academics saw that if they reported zero-days to BlackBox, the resulting fixes came out faster, giving them a quick and safe route to publication of their work. Within a year, a number of governments relaxed their policies on prosecution of hacking for research, on the understanding BlackBox would be used as a "clearing house". The BlackBox group responded by layering a cryptocurrency onto their mesh architecture, as a bounty mechanism for third-party contributions and a "proof of first report". Within two years the world had benefited from fewer breaches and a 70% drop in cyberattacks.

Related to: The Role of Government

What if …
government measures intended to protect networks made them even more vulnerable?

After Ten Years of a National "Intranet", Noorland Returns to the Open Internet

In a move welcomed around the world, Noorland's Prime Minister today announced she is reversing the country's Internet securitisation programme. In 2017, concerned about threats to national security and political stability, Noorland cut its networks off from the global Internet and kept almost all data and traffic inside its borders. Critics argued the extreme measure was actually aimed at opposition activists, not just at foreign hackers.

All data on Noorland citizens had to be held on servers physically located in Noorland, effectively banning foreign technology firms, and forcing all communications data through highly-controlled choke points susceptible to interception. The country's innovators and entrepreneurs complained that securitisation would cripple the economy, but the government insisted that security must come first.

Last month's devastating cyberattacks on the Noorland Internet showed how easily a concentrated network can be taken down. In an apparently coordinated series of attacks, node after node of the highly-concentrated network collapsed. Attacks came via multiple vectors and at different levels of the network, targeting local DNS servers, network gateways, and even bringing down for a short period the Tier 2 telecoms provider. It is not yet known if the attacks came from within or outside the country.

Most damaging of all, politically, was the hackers' broadcast on national television of a real-time graphical representation of the attacks. As the country watched, key nodes went down, one by one, live on-air. Viewers described an "almost apocalyptic" atmosphere as they watched single points of failure go dark.

The Prime Minister issued an edict immediately reversing securitisation, publicly recognising that her country had become powerless to prevent the very catastrophe that her digital sovereignty program was designed to stop. Today, she convenes the country's top Internet experts to work on making Noorland part of the global Internet, again, embracing the global Internet rather than shutting it out.

Related to: The Role of Government; Personal Freedoms & Rights

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if …
specialised networks and proprietary standards become the new norm?

Is the Internet Doomed? Open Standers Have the Answer

Alice Raven doesn't look like a revolutionary, but she speaks like one. At what turned out to be the final IETF meeting in 2022, the softly-spoken Singaporean presented some network graphs and diagrammes, lots of spreadsheets, and a few algebraic formulae. The big draw to her instantly-viral talk was its title: Is the Internet Doomed? Her answer: "Probably, but it doesn't have to be".

Raven's research proved what many had feared; thanks to global duopolies, opaque ownership structures, network traffic shaping, and the locking of 25% of the world's traffic inside national borders, today's global Internet is so concentrated, it has less than five points of potential failure. Raven recalled the IETF's glory days of open standards, protocols and free-flows of traffic — "this was an era of network optimism that we have clearly forgotten and sadly even derided".

Her generation grew up in an era of walled gardens, with standard setting usurped by the big Internet platforms. There is no Internet (with a capital I); now we have internets, she said, closed networks designed to extract revenues and choke off non-standard innovation. Raven's presentation closed with a rallying cry: The only way to return to the opportunity rich optimism of the early days of the Internet was to take action — it was time to say "No More" and return to the core principles of openness, global reach and interoperability.

Raven's walkout that day led several hundred engineers out of the meeting and into a new era. The "Open Standers", as they call themselves, are a loose group of engineers and programmers campaigning for radical network openness. They perform acts of construction and of resistance: one day building a community network in a South Asian megalopolis, the next, tearing open a globally branded IXP that sniffs packets from the starving north of Europe. Open Standers don't want to rebuild the old Internet, but to invent something even better.

"You could say we were radicalised", Raven says. "But by reality. That's how you know nothing short of revolution will work — when reality is completely broken".

Related to: The Internet Economy

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if …
the human body itself becomes the edge of an increasingly complex network?

Keynote Address of Tan Ai Lin to the First Joint Standards Meeting of the IEEE, IETF and World Health Organisation, Geneva, 2025

Some of you know my story, but here it is anyway. I'm Malaysian. I come from money. I am known for speaking bluntly.

With my background, I could have done anything. But my medical problems stopped that. Unstable epilepsy. Tachycardia. Exhaustion and mental fog. No fun! Basically, my wiring was wrong.

So, I thought it was time to be rewired. I put together the best team in the world. Instead of a pacemaker and drugs and never being 100% A-OK, I invented the Mesh. OK, joke. The people I hired did it. I gave the ideas, the money and the human body to work on. They got the Nobel. So, we're good.

The human body hosts trillions of microorganisms: three times as many non-human cells as human cells. You could say I have a bit more. Somewhere on the order of 3-4 trillion Nanodes. All talking to one another and all working to keep me ticking. It's like a wired up pleuritic membrane — the doctors here know what that is — that goes through my whole body. Genetically, let's just say I'm part electric eel. When I short circuit, twenty times an hour, the Mesh fixes it. I don't even feel it. Well, maybe I get a bit spacey. But it's ok.

I use a lot of bandwidth. I stream my data in real time, so any researcher can use it. Terabytes. I pull down A LOT of data to keep me working properly. It's like oxygen to me. Some people plan their vacations round the beach. I plan travel around low latency, high bandwidth. Lots of countries I'll never see. I can literally tell you how bad a crummy network feels. I'm a network edge all to myself.

A lot of my stuff is proprietary. Sorry about that. Openness is great. Speed is better. I wouldn't have chosen this way, but there was no alternative. I had to stay alive. But I'm here today because you guys have got to work together, right now. If you don't, we can't get this kind of technology out to everyone. And that would be too bad.

Related to: Digital Divides; The Internet & the Physical World; Media & Society

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if … the Internet of Things (IoT) is not based on open and interoperable standards?

Squabbling Siblings: Why My Light Bulbs Refuse to Talk to My Light Switch

Remember when technology was going to make life easier? Picture all those advertisements with smiling people tapping on devices that "just worked". OK, life's not like that. But must it be so complicated? Must I spend hours fiddling with control panels to make all the different parts of my house work together, and hours on the phone to customer support when they don't?

A month ago, I changed my energy supplier. The new one promised a lower rate and said there would be no problem replacing my smart metre with theirs. Now, I have indeed saved the price of a cup of coffee per month on my energy bill, but three mornings out of five I awaken to a cold shower.

You see, silly me, I should have known that my boiler would get offended and refuse to speak to the new smart metre. Then the smart metre would react by trying to bully the boiler into submission. Then the boiler would go on strike altogether. Ergo, no hot water for me, and the only savings on my heating bill coming from the fact that my radiators no longer work!

In technical terms, I am patronisingly told by my IT-literate teenaged son, the operating systems are incompatible. They are based on different and proprietary protocols developed by each company I deal with. Whatever that means. Is it unreasonable to expect the manufacturers to set aside their dreams of global dominance and concentrate on making products that, oh, I don't know, work?

Now, my son tells me, I must change the light bulbs. Soon, they won't work with the new system, either. Oh don't mind me. I'll just sit here in the dark.

Related to: Networks, Standards & Interoperability; The Internet Economy

What if …
the convergence of the digital and the physical worlds change what and how we eat?

Pervasive Connectivity and Big Data Slow Down Climate Change, One Beef Burger at a Time

By the 2000s, the industrialisation of food meant a single dish could contain elements from dozens of sources. But the food scandals kept coming: tainted infant formula, horse meat in beef burgers, and far worse. Regulation couldn't keep pace with opportunities along an ever-lengthening supply chain to make food cheaper, in worse quality and to fake its provenance for a better price.

The implementation in the early 2020s of nano-circuitry into sensors revolutionised both the physical resilience and the capabilities of what we then called the Internet of Things (IoT), in which everything, and everyone, could be networked.

IoT quickly found its way into the food production and supply chains delivering more efficient production, safer products and more comprehensive origin-to-destination tracking. Using IoT, the impact of food production on the environment became much more apparent through, for example, linking provenance records to measurements of environmental cost. Pundits and analysts started talking about an "Internet of Food" (IoF).

Perhaps unsurprisingly, the IoF's earliest adopters were not the industrial food giants, but artisanal foodmakers and organic farmers. Their premium products had suffered most in a market where consumers no longer trusted labelling.

Nowadays, every steak comes with a record of the animal's life, and detailed information on methane production and food miles. In the past five years alone, vegetarianism and veganism have doubled. Are meat avoiders driven by the severe weather events that are now our "new normal"? Or is it just harder to eat the leg of a lamb that was recently gambolling on a particular hillside? Either way, the IoF has increased production efficiency and reduced demand for the foods most implicated in climate change.

Related to: Media & Society; The Internet Economy

What if …
new ways to create and deliver content change not only the media but the business of sports?

Fly-Half with a Cool Billion; How Women’s Rugby Took Over the World

TimeMachine (TM) doesn’t actually stop time during play; it just seems like it. Top player Eve Mooney sets up a pass and time stops for the viewer. Will the centre pick it up or fumble it? Will the line-out go to the All-Blacks? TM’s AI pauses the stream and gives you a 360-degree view. You put a few cent on. The game restarts and you find out if you won. With realtime betting, you’re part of the drama.

Developed by two of the world’s top three media conglomerates, TM has changed sport as we know it, and now plays on devices held by 70% of the globe. But global media consolidation only explains so much. Why is TM rugby so addictive?

Sports Narratologist Anthony McDowell, who helped programme TM’s AI, explains why rugby dominates world sport; “Rugby was always a tactical game, but too fast. Set-pieces like scrums and line-outs pause the passing game and have a fixed number of outcomes, perfect for betting. TM ups the suspense and the stakes. You don’t get that in football. That’s why it’s dying”.

So why, of all the sports and cultures in the world, is women’s rugby at the top?

Mooney, the best-paid player in the world, has the answer.

“Money. TM means rugby makes more than all other sports combined. So that’s where the talent goes. And why women? The guys are too big. You can’t see the ball. Plus, they don’t think ahead so much. We always have, so it’s fun to bet on what plays I’m setting up, see if you can outthink me”.

Few spectators attend stadiums, now basically massive Faraday cages that lock down devices so you can’t communicate the results ahead of TM. And who would have predicted that the world’s biggest media groups, and not a state, got quantum cryptography working to protect its “live”-streams?

Related to: Artificial Intelligence

What if …
we use the Internet to drive transparency and strengthen democracy?

Follow the Money: How Open Everything Uses Radical Transparency to Keep Journalism Clean and Solvent

“Journalism was eating itself”, Jan Almeida tells me. “We needed to find a way to trust what we were reading and take responsibility as citizens for supporting real journalism. So we trained our own AIs to take apart the stories they push at us, and see what they’re made of. Sources, places, agendas, ownership. Everything. ”

We’re sitting on wonky chairs in a shared workspace downtown. Like their collaborators around the world, the loose collective that calls itself Open Everything works crazy hours in a scruffy-looking space full of soda cans, pizza boxes and white-boards covered in diagrammes and bad handwriting. Unlike many collaborative spaces, this one is completely fifty-fifty on gender lines, and the faces I see come in all the colours you see on the streets of this city.

“Sure”, Jan says, when I ask him if it’s intentional. “Equality isn’t something you sprinkle on the cake once it’s made. It needs to be baked in”.

Luisa Gomez, an older woman listening in as she writes code for a tool that tracks media ownership and political donations, interjects.

“We noticed, some years ago, that there was huge overlap between political extremism, online misogyny and dirty money”, she says, and grins. “It was almost as if the bad guys all knew each other”.

Jan winks conspiratorially then turns to me with a serious expression.

“Propaganda, financial secrecy, inequality and political polarisation — they’re all linked. It seems too big to fix, so you pick it off piece by piece. We build tools so anyone can understand what the agenda is behind what they’re reading …”

“But that’s not enough”, Luisa cuts in. “We also build up trust by helping people to support independent journalism. We make it easier to listen to the other side”.

“To all sides”, Jan agrees. “That’s the important thing”.

Related to: Personal Freedoms & Rights; Artificial Intelligence

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if …
the loss of trust in the Internet spurs a global movement of people disconnecting?

"Opting Out" Goes Mainstream

Anne meets me on a park bench in an affluent, middle-American city. It's swelteringly hot, but she wears a business suit and pantyhose. As we're in public, she also wears her anonymiser, a pair of spectacles that project a randomised set of features on her face. Anne's face can't be read by the recognition systems in every public and private space, so she's not getting location-based ads on her device. Nor can the "smart city" track her movements and raise an alert if she does something unexpected.

Facial anonymisers started as a tool for criminals and protestors, but are now worn by a growing-number of law-abiding citizens opting out of what they call "surveillance capitalism". It's not strictly against the law to opt out, but it's strongly discouraged.

"I'm a little unusual", Anne laughs. "Many opt outs get started because they're sick of ads or they've got a criminal record, so they're under active surveillance all the time. I've never broken a single law in my life. Not even jay-walking".

Anne seems too normal to live outside the technologies that protect us all. I ask what pushed her over the edge.

"Something bad happened to someone I love", she says quietly. "But there was a big protest that day. Some international summit. And nobody came to help her. Priorities, right"?

She fingers the device on her wrist. I realise with a shock that it's not a ubiquitous computing node, just a plain, old-fashioned watch.

"I looked at my device", she says, "and I thought, it's not just these companies tracking and manipulating me. Or the government. It's the whole thing. No one asked if I wanted it. They just assumed I'd … what do they call it? Trade off privacy for security. And I was OK with that. I thought they'd look after me when it really mattered. I trusted them".

She shakes her head in disbelief.

"But trust is a two-way street, you know? And from now on, I'm walking down it alone".

Related to: Personal Freedoms & Rights; The Internet Economy

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if …
algorithms dictate your ability to walk through the city?

Bigville's Super-Smart Algorithms Make Some Citizens De Facto Prisoners

It was a new era for Bigville; a "smart city" on a different scale, from centralised planning to better behaviour on the street. The world's first truly smart city went beyond just traffic management and cleaner air; it transformed each citizen's lived experience.

Smart policing applied evidence-based heuristics to real-time community support and protection, ending the divisive practice of "stop and search". Facial recognition, via the world's most dense CCTV network, made street crime almost impossible by profiling and tracking individuals the moment they step outside their homes. Individuals who trigger particular threat thresholds are followed, their every movement risk-assessed. This allows for police and emergency services to respond even faster to terrorism, crime and antisocial behaviour. Free from worries about disorder and mayhem, Bigvillers concentrate on what they do best: making money.

So what's gone wrong?

It turns out the profiling algorithms are becoming more focussed on factors that identify the wealthy from the poor, the cash rich from those in debt and the people who might be most likely to commit a crime. Shopping spaces use the same AI, allowing shop assistants to target those that are more likely and able to spend versus those just browsing. Public spaces and transport, building foyers and shopping areas monitor tens of thousands of individuals, tracking those with the highest risk profiles, with security on standby. Those identified as undesirable are discouraged from entering particular areas and buildings. The result is a growing segregation, with the poor actively managed away from affluent neighbourhoods and downtown areas because some unaccountable algorithm determines they have met or exceeded some threat threshold.

The city planners say the system just needs tweaking, and that algorithms are less discriminatory than humans, as long as the data is sound. But many, startled by Bigville's increasing use of profiling for the public good are asking whether the city, in becoming smart, has lost its soul.

Related to: The Role of Government; The Internet & the Physical World; Artificial Intelligence; Digital Divides

These stories show us how the Internet *might* evolve. But the path we take is up to us.

What if …
those who can't afford online security are divided into "haves" and "have nots"?

Data-Blockade of Chisnovia — Entire Country in Network Quarantine

In the first known instance of "network shunning", traffic exiting the landlocked country of Chisnovia is being identified and dropped by Internet Service Providers in its immediate neighbours — restricting cross-border traffic between Chisnovia and its neighbours. This is possible because recent changes to global networking protocols following unrelenting cyberattacks require all data packets to be geotagged.

Networking security expert Alex North told us the geotagged data packets can be spotted "like plague ships from long ago. They're waving the black flag that says they're infected, and we will burn them and all inside them before we'll let them dock in our ports".

In recent years, Chisnovia has been both the victim and the source of many volume-based and malware attacks. Despite warnings from the Regional Network and Information Security Agency (RNISA), the country has not cleaned up its cybersecurity act. RNISA's spokesman says the blockade is unofficial and is not RNISA initiated. The ban is believed to have been a business decision by the network of communications providers that control transit points in the region. The ISPs may have been influenced by the recent decision of a major insurer to invoke its terms on intermediary liability, holding them responsible for traffic that "could reasonably be expected" to be high risk.

An unnamed official in the Chisnovian justice ministry complained; "In 2004, we had two computers in the whole ministry. Then "development experts" fixed our so-called digital divide by networking everything in the country. So now we're supposed to gratefully spend millions securing it? To keep rich foreigners' systems free of the inconvenience of spam and DDOS or malware attacks while we can barely afford to run our prisons or hospitals? Forget it".

Related to: Cyber Threats; The Role of Government

What if … the way we invest in access perpetuates the global digital and socioeconomic divides?

Digital Opportunity – Winners and Not-Quite-Winners

“I hate that place”, Angel gestures at the vast, low-rise data centre crouched behind barbed wire.

The fence runs hundreds of metres along an empty road. We’re twenty kilometres from the city. In a country where 40% of the population is still offline, this former plantation runs fibre optic cable straight to the country’s main Internet exchange.

Angel leans out of the four-wheel drive to point at the huge “Keep Out” sign.

“Sometimes I drive out here on my scooter and just look at it. I think about burning it down”.

I say that sounds kind of extreme.

“OK”, Angel says, in his Hollywood-accented English. “Where I live, we get brownouts all the time. Black-outs, too. You can’t build anything that’s gonna change your life on maybe six hours of power a day”.

“But you’ve got access, right”? I ask.

“When the power’s on we get 56k dial-up”, Angel says. “You even know what that is”?

“I’m from New York and I’m under forty”, I laugh. “I have absolutely no idea”.

“You dial up each time you want to connect. There’s no “always on”. And it drops out. All. The. Time. I design a website, I’m uploading pages and boom. It’s gone. Start again”.

“That sounds frustrating”, I say.

Angel jerks his thumb at the data centre.

“But in there, lights are always on. They ration broadband from the exchanges to, like, fifty connections, and that’s one of them”.

“So”, I say, “It looks like opportunity, but it’s not”?

“They get the energy”, he says. “The tax breaks. You know there are maybe three people working in there? But when it opened, the whole government got their pictures taken. It’s like, they get the cream and we’re just …”

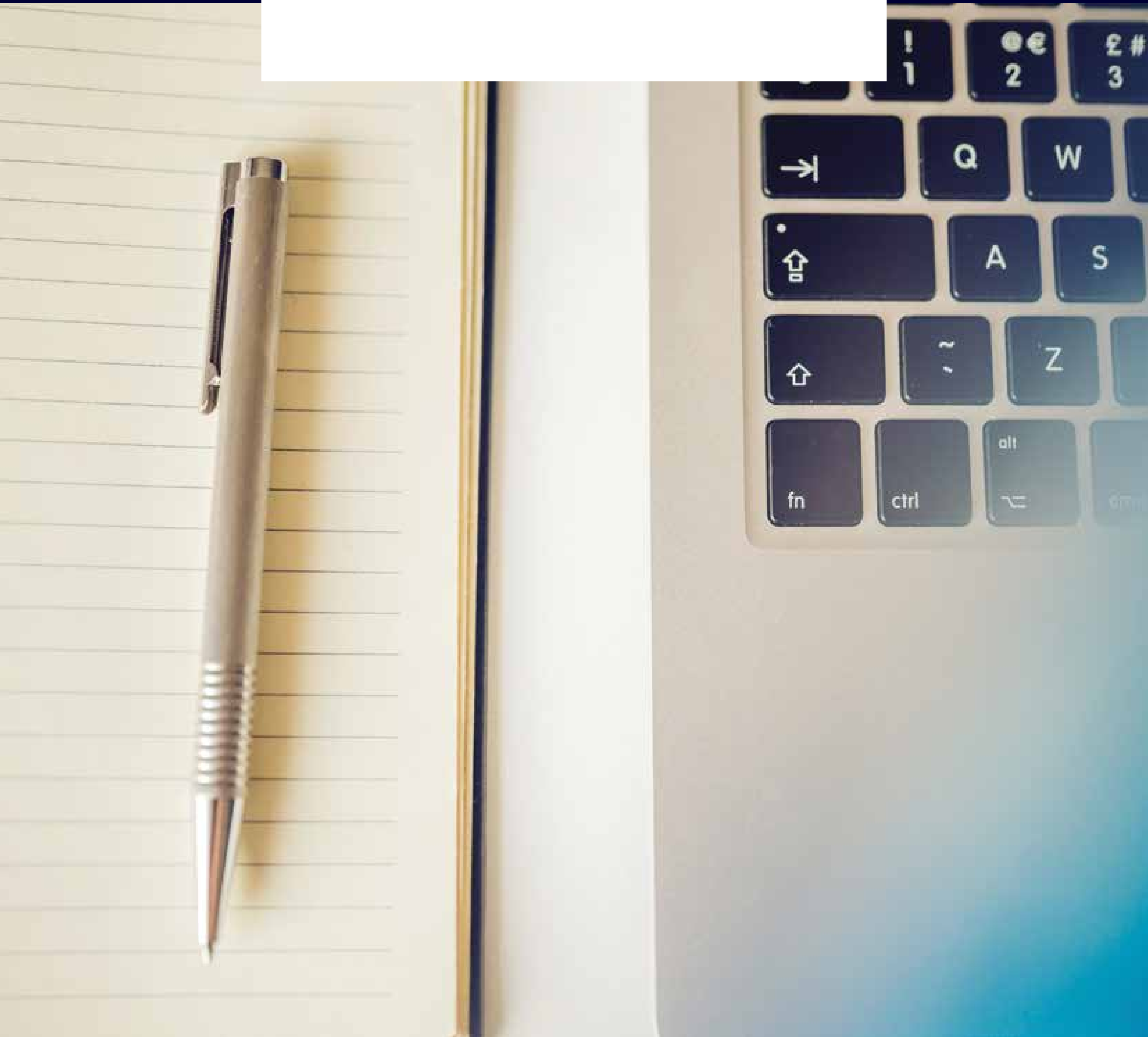
He pauses and takes a deep breath.

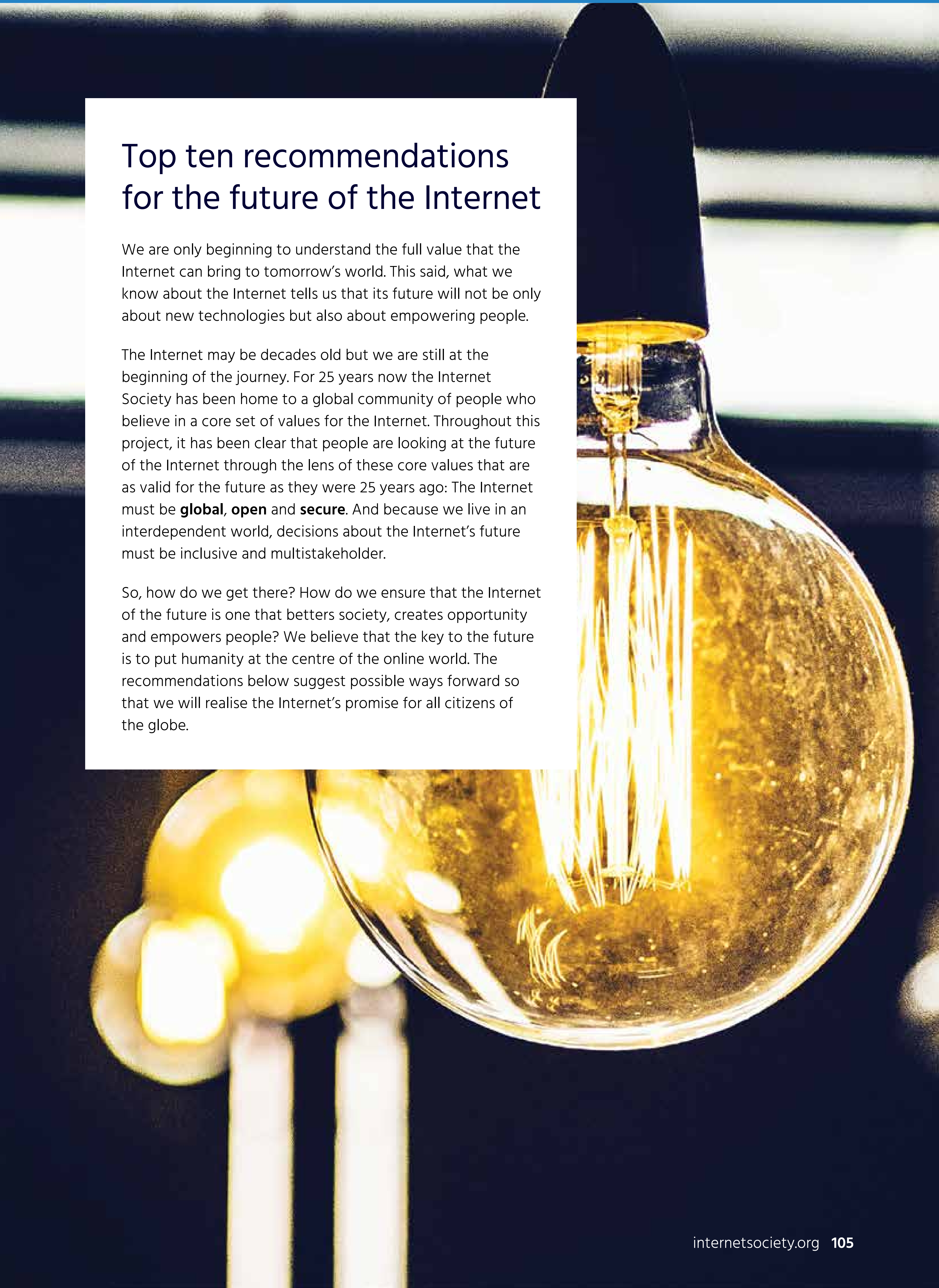
“It makes me mad”, he says, quietly. “It makes me want to do something”.

Related to: The Internet Economy

9

Recommendations





Top ten recommendations for the future of the Internet

We are only beginning to understand the full value that the Internet can bring to tomorrow's world. This said, what we know about the Internet tells us that its future will not be only about new technologies but also about empowering people.

The Internet may be decades old but we are still at the beginning of the journey. For 25 years now the Internet Society has been home to a global community of people who believe in a core set of values for the Internet. Throughout this project, it has been clear that people are looking at the future of the Internet through the lens of these core values that are as valid for the future as they were 25 years ago: The Internet must be **global**, **open** and **secure**. And because we live in an interdependent world, decisions about the Internet's future must be inclusive and multistakeholder.

So, how do we get there? How do we ensure that the Internet of the future is one that betters society, creates opportunity and empowers people? We believe that the key to the future is to put humanity at the centre of the online world. The recommendations below suggest possible ways forward so that we will realise the Internet's promise for all citizens of the globe.

Human values must drive technical development and use

- We must have a public debate for society to agree on ethical standards and norms for the use of emerging technologies.
- These ethical considerations should be embedded in the design and development of new technologies.
- Industry should be proactive in incorporating independent ethical reviews into business decisions about emerging technologies.

Apply human rights online as well as offline

- Governments should stop using Internet shutdowns and other means of denying access as a policy tool: we must keep the Internet on.
- Just as in the offline environment, any limitations to human rights online should be a last resort and be exceptional, proportionate and follow the due process of law.
- Individuals should continue to have the ability to communicate confidentially, anonymously and securely.
- Encryption is and should remain an integral part of the design of Internet technologies, applications and services. It should not be seen as a threat to security. We must strengthen encryption, not weaken it.

Put users' interests first with respect to their own data

- Put users in control of their own data. All users should be able to control how their data is accessed, collected, used, shared and stored. They should also be able to move their data between services seamlessly.
- Application and service providers must be transparent about how and why they collect users' personal data. No one should use personal data to discriminate against individuals or groups of individuals.
- Encourage data minimisation practices. Insist on selective data collection and only for as long as necessary.

Act now to close digital divides

- Recommit the UN Sustainable Development Goals, in particular, to provide universal and affordable access to the Internet in least developed countries by 2020.
- Prioritise infrastructure development around the globe including high speed and wireless networks, community-based infrastructure and data centres.
- Create a hosting environment for local content that reduces transit costs and allows for cheaper, better, faster traffic exchange.
- Equip youth and workers with the right skills, connect local talent to the global economy.
- Incorporate security-by-design into devices and systems to prevent the emergence of a security divide.

Make the Internet economy work for everyone

- Governments, insitutions and industry must prioritise skills development and training to allow people to keep pace with innovation and its impact on jobs. They must prepare the workforce for “new collar jobs”.
- Create an enabling environment for entrepreneurship and empower people to create their own globally competitive startups Ensure users from all around the world become creators rather than simply consumers.
- Remove barriers to cross-border data flows to ensure that everyone has the same opportunity to participate in and benefit from the global Internet economy.
- Competition policies across the world should be adapted to reflect the complexity of the modern Internet economy, including taking digital presence, data collection and citizen use into account when assessing a company’s market power.

Take a collaborative approach to security

- Online security must be made easier for users. Industry and governments should invest in the creation of usable tools and information to help users make informed decisions about privacy, rights and security.
- Corporations and governments must adopt a risk management approach that goes beyond securing infrastructure and incorporates the principles of responsibility, collaboration, and the safeguarding of human rights. They must develop best practices to protect their networks from Internet threats, and protect the Internet from vulnerabilities on their network.
- Security professionals must work collaboratively to test product security and disclose any vulnerabilities in a responsible manner. The cost of security failures must be assessed to those who cause the failure, not to the end user.
- Legal and policy frameworks must allow ethical hackers and penetration testers to share information.

Increase accountability for data handlers

- Create an accountability regime, including liability provisions to ensure that those entities that collect, compile and manipulate data are liable for its abuse and its security, not the users.
- Develop insurance policies that reward responsible security behaviour and the proper protection of personal data.
- The roles, responsibilities, and liabilities of those handling data should be clarified.

Build strong, secure, resilient networks

- Interoperability based on open standards, global reach and integrity, and permissionless innovation must remain a cornerstone of future network development.
- Technologists need to promote diversity in networks and services to allow for the next generation of products and services to emerge.
- Prepare for dramatic growth in the number of users and devices. Scale bandwidth and IP addressing capability by investing in underlying network infrastructure including IPv6, as well as new radio equipment and technologies (e.g. 5G), and backhaul fibre.

Address the need for online social norms

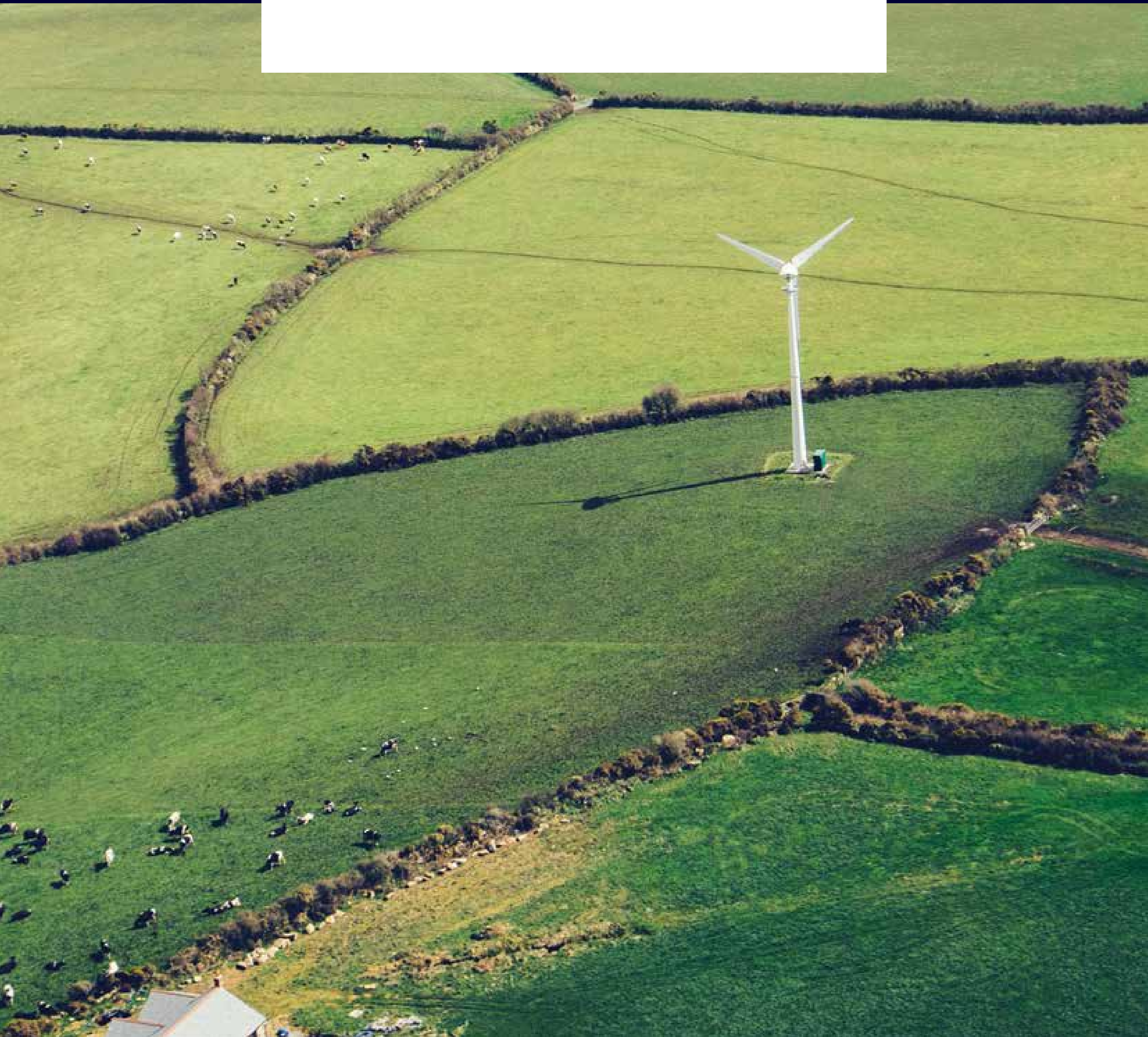
- Make the Internet a safe place where everyone is free from online violence and harassment.
- We must forge basic norms of behaviour online so that users feel confident in using the Internet.
- Large Internet platforms must take greater responsibility to tackle the problems of violence and hate online.
- Multistakeholder engagement is the way to develop norms of behaviour. All stakeholders in society need to accept responsibility to ensure that the Internet is not used as a tool to spread hate.

Empower people to shape their own future

- Stakeholders should support civil society and its critical role in protecting and promoting human rights online.
- Governments should welcome and support civil society's meaningful participation in domestic Internet policymaking.
- All stakeholders should build momentum from the recent success of multistakeholder processes, and expand the use of these processes globally.

10

Conclusion



No one knows exactly how the Internet will evolve. We do know it will require new thinking, new approaches and new tools to adapt to this rapidly changing world.

People often make the assumption that the Internet will simply always be there; always on, serving our needs in a rapidly-shifting digital world. The reality, however, appears in stark contrast to this idea.

We have seen, through the many voices and perspectives reflected in this report, how those most closely connected with the origin, growth and development of the Internet are unsure, even fearful, for its future. They know that there are no guarantees for what lies ahead, only questions that need answering. They reflect the belief that if future generations are to continue to be able to interact with the digital world, then we need to be much more conscious of the path that we are creating today for the Internet of tomorrow.

One of the main ambitions with this project has been to illustrate these uncertainties surrounding the Internet's future. We have done this by looking at the interdependencies that exists between key driving forces of change and what they mean for some of the most important aspects of our society. From market developments to cyber security, to the relation between new technologies and the actions of governments, the possible outcomes are as varied as they are unknown.

Indeed, nothing is certain, but in the process of surveying and interviewing the community, a number of defining themes came the fore. Three in particular stand out.

1. Optimism and disillusionment exist in equal measure

There is a general sense that while the Internet still offers great opportunity and that many, particularly in the developing countries, see the Internet as an important means to empower communities, there is also a strong sense of disillusionment with what the Internet brings. The tool that was, in the words of one participant, "supposed to democracratise society" is now being used as a means for its control. This disillusionment is felt even more profoundly in developed countries where the Internet is on the cusp of changing significantly through new technologies and persistent security challenges.

2. We need to reassess what we believe we know

We have learnt that we can no longer afford to think about the Internet and its opportunities and challenges as we used to do. Technologies such as the Internet of Things and Artificial Intelligence are set to redefine our understanding of the world around us, reshaping economies and societies in unprecedented ways and necessitating *new thinking, new approaches and new models* to address a range of emerging issues.

3. People come first

The third, and perhaps most important theme running through the responses is the imperative of *putting the human, the user, first.*

Above all, there is an unshifting conviction that the Internet must continue to benefit people and create new social and economic possibilities, thereby fulfilling the premise on which it was built. Hyperconnectivity promises to reshape business, public services and other entities through greater efficiencies, immediacy, reach and delivery. With more comprehensive and effective data collection, analysis and use we can expect revolutionary change to come to healthcare, education, and other services, but none of this will be of any value if people are not the ones that benefit.

This report never set out to predict the future. Rather, by listening to the views of those who are part of the global Internet community, it serves as an indicator for the vast range of possibilities that exist. Whether it's understanding the future as an overwhelming range of "domino effects", or as a chessboard of actions and reactions, no reality today allows us to fully grasp a future that we have yet to see. The unknowns about technological development and the actions of various stakeholders are all the as-yet-undefined determinants of the Internet of tomorrow.

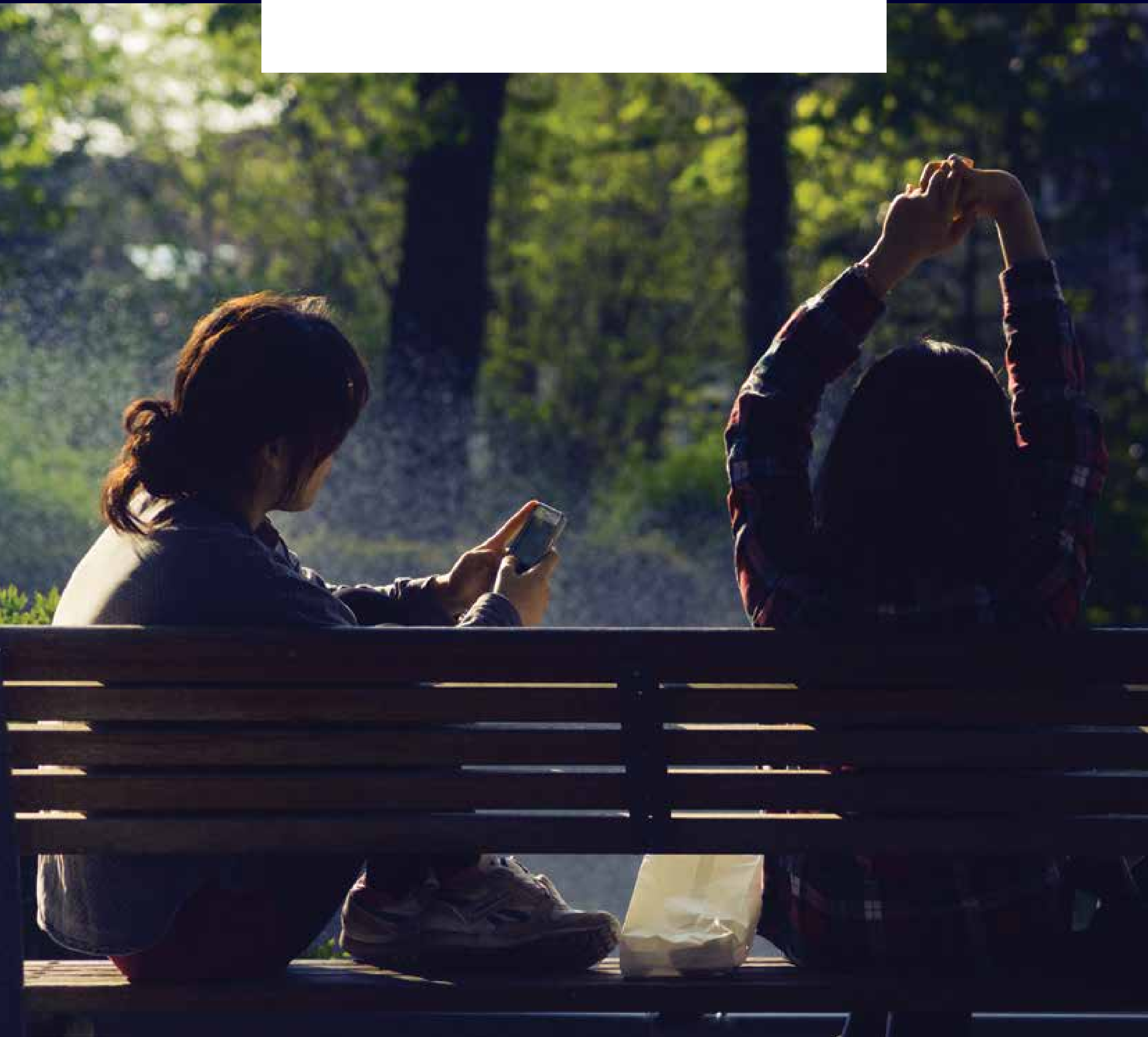
What *is* certain however is that there is a lot to do to keep the Internet on course to remain open, globally connected and secure. These core principles that have allowed the Internet to flourish as a tool for human empowerment have allowed people to connect, share, innovate and improve their lives. Throughout this project, it has been clear that people are looking at the future of the Internet through this lens. They all ultimately connect back to a vision where the Internet's capacity to promote human empowerment is preserved.

Achieving this vision in the years to come depends on collective action. We need a different mindset that helps us move from managing disruption to the way things are today, to inventing new frameworks for anticipating and managing the way things will be. To do that, we must have inclusive discussion and decision-making and we must think harder about the future together. Indeed, solutions to the changes occurring in our societies today may not be at all obvious because we have not yet done the work to fully adapt to our present circumstances.

The future of the online universe is ours and ours alone to shape. We can start by making decisions that preserve the values that underpin the Internet we know today.

11

Methodology



Methodology

In 2016, the Internet Society initiated a process to elicit opinions and perspectives from the global Internet community (e.g. Internet Society members and staff, Internet luminaries, policymakers, technologists, academics, business leaders, as well as Internet users around the globe) about the key forces of change (both emerging trends and key uncertainties) that they believed would drive the future evolution of the Internet. The analysis and consolidation of these opinions and perspectives form the core of the findings in the 2017 Internet Society Global Internet Report: Paths to Our Digital Future.

The process of gathering the community's views on the future of the Internet comprised a number of elements:

- In-depth interviews of over 130 Internet experts and users
- Two global surveys that received over 2,000 responses from around the world and across all stakeholders
- Two regional surveys
- Ten Internet Society community roundtables
- A survey soliciting suggestions for recommendations as to future actions

In total, more than 3000 survey responses were received. Responses to the two global surveys came from 160 countries and 21 regions around the world. Individuals from approximately 94% of the Internet Society chapters participated in the surveys, and 69 per cent of respondents self-identified as Internet Society members.

Interviews

More than 130 experts from a diverse group of stakeholders, including governments, civil society, businesses, academia and the technical community were interviewed at length. The interviews solicited views on how the Internet had changed over the past five years and on the Internet trends and uncertainties for the next five to seven years. To encourage the most robust set of views on the future of the Internet, the questionnaire used the term "Internet" in its broadest sense, encompassing everything from its structure, governance, and underlying technologies to access, usage, and connected devices. The interviews took up to an hour to complete.

The main section of questions asked respondents to describe the greatest forces of change, including predictable trends, as well as key uncertainties, that they believed would affect the future of the Internet over the coming five to seven years. Respondents were asked to provide these forces of change in each of five categories: Social, Technological, Economic, Environmental, and Political (STEEP). The last set of questions respondents were asked revolved around what they believed to be the most ideal scenario for the future of the Internet, the most pessimistic scenario for the future of the Internet as well as the greatest questions they still have around the future of the Internet.

Examples of questions included: "What trends (i.e., highly predictable forces of change) are you starting to see develop that will likely affect the future of the internet over the coming five to seven years? How do you see these trends playing out"? And, "What are the greatest uncertainties (i.e., issues we know are important but are difficult to predict) that you could see impacting the future of the Internet? How could these unfold in different ways — and what impact would each have on the future of the Internet"?

Global surveys

The interviews were complemented by two global surveys over the course of several months in 2016, with the intent to gather qualitative and quantitative data from stakeholders, experts, and Internet users around the world on the key forces of change driving the future of the Internet.

The first survey was comprised of open-ended questions in order to solicit input in parallel with the interviews, and was used to identify the set of issues that our global community believes will drive change in the Internet in the future. From transformations of the Internet economy to the crippling effects of cyberattacks, 309 unique forces of change impacting the future of the Internet were identified. Through grouping of similar concepts and a screening based on impact and predictability of forces, Internet Society staff merged these 309 forces into a smaller subset of 37 uncertainties that formed the basis of Survey 2.

The second survey was targeted at gathering opinions on the likely direction (or inherent uncertainty) of these key forces of change identified in the first survey. These issues (or forces of change) were provided to survey respondents along with two sliding scales — one representing today, and one representing 2021. Respondents were asked to place a marker between two plausible extremes of how the issue could unfold, with the mid-point reflecting uncertainty. By comparing the placement of the market between the 'Today' and '2021' sliders, we were able to gauge the direction of change.

The findings from the interviews and surveys were further consolidated into the six Drivers of Change and three Areas of Impact that guide this report.

Roundtables

The Internet Society organised over 10 roundtable discussions with our community from different regions to discuss in greater depth the initial findings. These included the following events/discussions:

- Internet Society Board of Trustees, 2016
- Internet Hall of Fame members (multiple video conferences)
- Internet Governance Forum 2016, Open Forum
- IETF Policy Makers Roundtable
- IETF 95 & IETF 98
- Internet Society all-staff meeting, 2016
- Internet Society Organisational Members Briefing, IETF 98
- RightsCon Brussels 2017 Chapter calls: Youth SIG, Africa (English & French), Latin America
- Chapter meeting, Oman
- Caribbean Chapter roundtable, ARIN 39

Regional surveys

In order to ensure that there was greater depth of information from Asia-Pacific and Africa, we followed up with two surveys to supplement the regional input on the emerging security and trust divide, and artificial intelligence.

Interview questions

1. Do you see a linkage between cybersecurity/ cybercrime and peoples' ability to access and use the Internet?
2. To what degree will trust impact peoples' ability to access and use the Internet? Will there be a difference between or within countries?
3. What do you think the policy responses from governments to cyberattacks will be?
4. How will government responses to cyberattacks impact the open Internet?
5. How will governments respond to the increased use and deployment of Artificial Intelligence and the Internet of Things?
6. What are the implications of the above for society?

Recommendations survey

In June 2017, the Internet Society issued a final survey to seek input on a set of recommendations to address the challenges and opportunities identified in the Drivers of Change and Areas of Impact. These served to complement and inspire recommendations developed by Internet Society staff.

12

Acknowledgements

Acknowledgements

The 2017 Global Internet Report reflects comments and insights from across the Internet Society community and well beyond, including global and regional partners, Internet pioneers and experts around the world. We appreciate the extensive contributions of our Board of Trustees, Chapters, Organisation Members, members, and staff who shared important perspectives for this report.

We would like to thank Kathy Brown, Sally Wentworth, James Wood, Olaf Kolkman, and Raúl Echeberría for their leadership and support. A team of staff members, led by Sally Wentworth, dedicated more than 18 months to collecting data, organising and refining the findings and writing the final report. Special thanks to James Wood, Carl Gahnberg, Mark Buell, Constance Bommelaer, Wende Cover, Ryan Polk, Greyson Nevins-Archer and Nicole Carolin for their commitment to this initiative.

Matthew Shears, consultant for the Internet Society, served as the lead writer on the report, and we greatly appreciate his extensive work to bring this report to completion. Special thanks to Karen Rose who initiated and was a guiding force for this project through 2016, and to Heidrick & Struggles for their support in the data collection and analysis.

Thank you to our staff subject matter experts for their invaluable comments and suggestions: Robin Wilton, Raquel Gatto; Steve Olshansky, Sebastian Bellagamba, Christine Runnegar, Nicolas Seidler, Andrei Robachevsky, Rajnesh D. Singh, Dawit Bekele, Jane Coffin, Joyce Dogniez, Elizabeth Oluoch, Mat Ford, Salam Yamout, Frédéric Donck, Jairus Pryor, Naveed Haq, Konstantinos Komaitis, and Niel Harper.

We would also like to thank the Internet Society IT and communications teams for their support in creating the online and print versions of the report, as well as promotion, media outreach and many other activities to launch the report. Thank you to Adnan Nawaz for his excellent work on the video production, Yoko Co as our web design partner, Rachel Ingram and Grant Gross for their editing, and Maria Farrell as the creator of the fictional vignettes and editing work.

Internet Society

About the Internet Society

The Internet Society is a global cause-driven organisation governed by a diverse Board of Trustees that is dedicated to ensuring that the Internet stays open, transparent and defined by you.

We are the world's trusted independent source of leadership for Internet policy, technology standards, and future development. More than simply advancing technology, we work to ensure the Internet continues to grow and evolve as a platform for innovation, economic development, and social progress for people around the world.

With offices around the world, we work to ensure that the Internet and the web that is built on it:

- **Continues to develop as an open platform that empowers people** to share ideas and connect in new and innovative ways
- **Serves the economic, social, and educational needs** of individuals throughout the world — today and in the future

Learn More About the Internet Society at
www.internetsociety.org

Join the Internet Society and get involved
www.internetsociety.org/get-involved