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].

Cyber Threats

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.