CHAPTER 10

Fundamentals of cyber security

Dave Clemente

Introduction

Cyber security is an increasingly relevant and pressing area of concern for individuals, companies and governments, and one that is hard to ignore. This chapter looks at primary factors that make cyber security both important and difficult to achieve. Analysis begins by looking at the evolving digital environment, continues with an examination of dynamics that make cyber security so challenging, and concludes with a look at possible futures.

The goal of this analysis is to cut through the hype that surrounds cyber security and to provide the reader with a clear yet nuanced perspective of what is important and why. This is a challenge when fundamental concepts are often poorly understood and where there are strong commercial and political incentives to exaggerate perceived dangers.

To understand what is meant by 'cyber security' it is helpful to begin by looking at a definition of cyberspace:[1]

> Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our companies, infrastructure and services.[2]

Cyberspace can be divided into a multi-layer model comprised of: [3]

1. *Physical foundations:* such as land and submarine cables, and satellites that provide communication pathways, along with routers that direct information to its destination.
2. *Logical building blocks:* including software such as smartphone apps, operating systems, or web browsers, which allow the physical foundations to function and communicate.
3. *Information:* that transits cyberspace, such as social media posts, texts, financial transfers or video downloads. Before and after transit, this information is often stored on (and modified by) computers and mobile devices, or public or private cloud storage services.

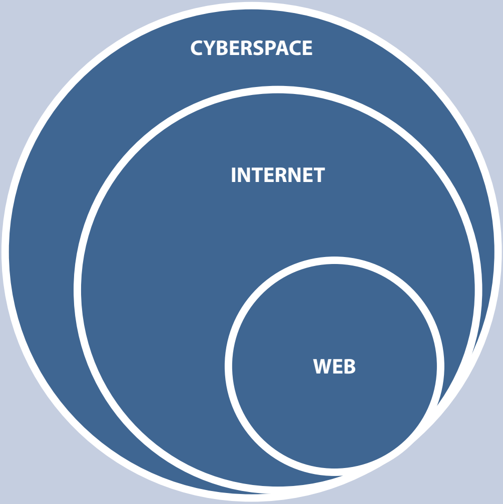
4. *People:* that manipulate information, communicate, and design the physical and logical components of cyberspace.

Collectively these tangible and intangible layers comprise cyberspace, which we are increasingly dependent on for essential components of daily life. A dependable and stable cyberspace is necessary for the smooth functioning of critical infrastructure sectors such as energy, transport, food, health and finance. As dependence increases, so do the costs of disruption—whether accidental or intentional—as well as possibilities for misuse and abuse.

The web is not the internet

When cyber security is mentioned, many people tend to think of the security of their devices, home or work computers, or the websites they visit on a daily basis. But cyberspace is much larger than this (see Figure 1 below) and includes the sum of global digital networks. It includes all digital communications including obscure and legacy communication protocols or isolated networks (for example, nuclear weapons silos) that are not accessible through the internet. The internet (the IP—or Internet Protocol—network) is a slightly smaller circle that includes the most popular and widely used forms of communication.[4]

Figure 1 Overlapping systems of digital communication



Inside the internet is yet another circle—the web, or the pages that can be accessed using a web browser such as Firefox, Chrome or Safari.[5] The internet and web are often used interchangeably, but in fact they are different and one of them sits inside the other. Although this chapter (and most popular commentary) talks about cyber security, what is really meant is security of the internet, where the vast majority of global communication takes place.

Author and journalist John Naughton provides a useful analogy to describe the difference between the internet and the web:

> Think of the internet as the tracks and signalling, the infrastructure on which everything runs. In a railway network, different kinds of traffic run on the infrastructure—high-speed express trains, slow stopping trains, commuter trains, freight trains and (sometimes) specialist maintenance and repair trains.
>
> On the internet, web pages are only one of the many kinds of traffic that run on its virtual tracks. Other types of traffic include music files being exchanged via peer-to-peer networking, or from the iTunes store; movie files travelling via BitTorrent; software updates; email; instant messages; phone conversations via Skype and other VoIP (internet telephony) services; streaming video and audio; and other stuff too arcane to mention. [6]

Cyberspace in context

The four layers of cyberspace described above (physical, logical, information, and people) have three primary characteristics—connectivity, speed and storage. These characteristics enable both the positive and negative aspects of the digital environment and should be understood in order to place cyberspace in context. This is also how readers can begin to understand cyber security—by examining the basic layers of cyberspace and their characteristics and analysing what this means for the safety and stability of the modern digital world.

Connectivity

Nearly 40 per cent of the world's population is connected to the internet, through PCs, laptops, tablets and mobile phones. In addition, there are billions of other connected 'things' such as sensors embedded in cars, factories, buildings, airplanes, TVs and toasters. This rapidly increasing connectivity produces value and benefits that are more than the sum of the individual parts. This is known as a positive 'network effect'—as more devices are connected, more information is generated and shared, and the value of the network increases for everyone.[7]

There are clear benefits, for example, from being able to email anyone around the globe who connected to the internet, as opposed to being restricted to Western Europe. The value of social networks, such as Facebook or LinkedIn, increases dramatically as more people join. Widespread connectivity also helps to identify trends and activities that were previously very difficult or impossible to spot, such as tracking the spread of infectious diseases.[8]

Connectivity allows text messages and documents to be sent reliably around the globe almost instantaneously, making distance irrelevant. This connectivity is good for employees working from home or students checking Facebook from a coffee shop, but it is equally good for hackers attempting to break into a computer on the other side of the world, or knock websites offline using the computing power of a botnet (that is, a group of computers that have been infected with malicious software).[9]

Speed

Why does cyberspace seem to change so quickly, presenting opportunities and challenges at greater speed than we are accustomed to in the physical world? There are a number of reasons for this change, and they are scattered throughout the twentieth century. They include the inventions of the semiconductor and transistor.[10] Steady advances in technology led Gordon Moore (co-founder of Intel) to state his belief that engineers would be able to double the number of transistors on a computer chip every two years.[11] This observation, known as Moore's Law, was made in 1975 and has held true for the past four decades. It means that the speed—processing power—of computer chips increases steadily, making laptops more powerful, turning smartphones into handheld computers, and allowing Google searches to be completed ever-faster. Squeezing more transistors onto a chip means greater speed, and speed underpins the digital world.

Storage

Greater connectivity and speed are nice, but they mean little without storage. What good is an email, text, spreadsheet or document if it can be sent and received, but not stored and retrieved? Storage capacity has come close to matching Moore's Law (namely, doubling roughly every two years) as hard drives have moved from gigabytes to terabytes and continue to grow.

Storage involves not only capacity, but also performance, which is the input/output speed of a storage device. Performance has increased dramatically with the transition, over the past decade, from traditional hard drives with spinning discs to solid state hard drives that have no moving parts—the same storage in smartphones and flash drives. Storage allows internet users to download and retain music, videos, pictures and much more. This is equally valuable for attackers who are looking for large repositories of information, or who wish to siphon large quantities of information from compromised networks.

Dependence and dual-use

The effects of this connectivity, speed and storage are many and varied, but at least two implications can be identified. First, the modern world is heavily dependent on digital technologies, often in ways that are subtle or not readily apparent. The internet facilitates the vast majority of digital communications, including financial transactions, telephone and video calls, and text messages. Critical infrastructure sectors such as food, transport, and water rely on digital connectivity to increase efficiency and profits. As James Lewis noted: 'the effect of the internet is to lower transaction costs—everything else is just advertising'.[12] This dependence on the internet as the central nervous system of the globe is growing steadily and shows no signs of slowing.

> We don't have cars anymore; we have computers we ride in. We don't have airplanes anymore; we have flying Solaris boxes attached to [many] industrial control systems. A 3D printer is not a device, it's a peripheral, and it only works connected to a computer. A radio is no longer a crystal: it's a general-purpose computer, running software.[13]

Second, all technologies are dual-use. There are no kinds of connectivity, speed or storage that will only benefit desirable actors and exclude undesirable ones. The benefits of this environment, for example, the ability to innovate without asking permission from anyone, are available to all actors, malicious or benign. This crucial point is often overlooked by policy-makers who attempt to impose technological solutions to societal problems as they ask 'can't you just make us a general-purpose computer that runs all the programs, except the ones that scare and anger us? Can't you just make us an internet that transmits any message over any protocol between any two points, unless it upsets us?'[14]

Cyber security in context

The three characteristics discussed above—connectivity, speed, storage—have been combined to create many opportunities but also threats. As the global economy becomes more dependent on the internet, and as attacks and data breaches become more costly, cyber security is receiving more attention from decision-makers in the public and private sectors.

Cyber security is about protecting the confidentiality, integrity and availability of information—whether it is personally identifiable information, email or other kinds of communication, credit card numbers, intellectual property or government secrets. Hackers, organised criminals, commercial competitors and government intelligence agencies are increasingly active on the internet and engaged in various kinds of theft, disruption, espionage and sabotage.

Defending computer networks and protecting information from these actors is a difficult and ever-changing task. Defenders must protect against all known vulnerabilities, while attackers only need to find one unprotected vulnerability (or discover a new one). The process of securing digital networks and information is a balance between competing priorities—investing in cyber security or, for example, expanding into new markets. It involves risk assessments of the kind that are familiar to decision-makers in the public and private sectors. However, these risk assessments are becoming more difficult as the digital 'attack surface' grows exponentially, and as connectivity spreads beyond PCs, laptops, and smartphones to include low cost, low margin devices.

These devices can now be placed into almost any device or location, allowing household appliances, cars, medical implants, and even farm animals to be connected to the internet.[15] The information that is generated or transmitted by these devices may be the target of attacks, but the software that runs them may also be the target.

All modern economies depend on software to operate transportation, communication, and energy networks along with many other aspects of daily life. Good software is difficult to create, and pervasive vulnerabilities make our computers crash inadvertently, allow hackers to evade detection and defraud our bank accounts, or government spies to secretly collect vast quantities of information. These vulnerabilities permeate computer networks and are a symptom of larger problems.

> Everything is broken [. . .] Software is so bad because it's so complex, and because it's trying to talk to other programs on the same computer, or over connections to other computers. Even your computer is kind of more than one computer, boxes within boxes, and each one of those computers is full of little programs trying to coordinate their actions and talk to each other. Computers have gotten incredibly complex, while people have remained the same grey mud with pretensions of godhood.[16]

These vulnerabilities pose a risk to personal information, intellectual property, government secrets and, potentially, to the infrastructure that underpins the internet. The cyber security community has consistently been outpaced by technological developments and, in a business environment, often struggles to articulate why spending on cyber security should take precedence over activities which more directly contribute to commercial profitability. Many proposals have been made to change this dynamic, from vendor liability for producing or selling insecure software to bonuses (instead of legal threats) for security researchers who uncover technical vulnerabilities, but little progress has been made. The pessimist would note that change is likely to come only after a large and damaging incident. The optimist would observe that, in spite of pervasive weaknesses, the digital environment functions well enough to serve as the nervous system of the global economy and financial markets.

Stability and shared interests

Significant investments have been made to ensure the reliable functioning of the internet, particularly by the companies that own the physical and logical infrastructure, and the result has been relatively few significant or sustained disruptions. In part this could be attributed to the benefits that all actors gain from an ever-expanding digital environment. For the benign actor the benefits include increased social and economic possibilities, as they can more easily shop online and communicate with friends and relatives around the world. For most malicious actors there is little incentive to disrupt the functioning of the internet. After all, the spread of connectivity means more naïve individuals who can be defrauded, and more computers that can be hijacked and used for profit.[17]

One major change over the past twenty years is the growth in global economic interdependency. This is a reliable stability mechanism and one that is reinforced by the growing use of the internet. Financial transactions, communication channels, media and entertainment networks—all of these transit the globe at the speed of light, with little regard or respect for the inflexibility of geographic boundaries.

Shared dependence on the smooth functioning of the internet means there is reduced incentive to destroy or disrupt it, as hackers and criminals would suffer along with everyone else. For governments, economic interdependence increases the costs (to everyone) of overt offensive action in cyberspace, and this has resulted in the steady growth of covert activities.

There are strong economic incentives to connect to the internet, and even stronger incentives to disconnect. Even when intentional disconnections take place, they cannot be sustained for long. The Egyptian government shut-off the majority of the country's internet during the Arab Spring (except for the connections that allowed the Egyptian stock market to continue functioning) but it could not sustain this action for more than five days.[18]

Financial connections entangle nearly every country in the world, and mutually assured nuclear destruction has been replaced by mutually assured economic destruction. For example, sanctioning Russia for its military actions in Ukraine by cutting it off from SWIFT (the global financial messaging system that clears trillions of dollars per day) would be a serious escalation that would cripple Russian banks and be costly for foreign banks with investments in the country.[19]

Government limitations

There are strong shared interests in cyberspace at the international level, primarily focused on maintaining operational stability, but there are also conflicts of interest and areas where government power is limited. Cyber security has characteristics that set it apart from traditional security and defence, making it both interesting and difficult. It is difficult for governments to accept that they are not always the most powerful actor, and that they must rely on the private sector to gain better situational awareness or to access skilled people and innovative technologies.

Governments and companies have access to different pieces of the cyber security puzzle, such as network traffic, threat intelligence or human resources, which they sometimes share with each other in private forums. This sharing can be mutually beneficial, but the essential ingredient—trust—is hard to build and easy to destroy. Information-sharing is most effective when there are common mutual interests, when cooperation is narrowly focused and limited in duration, or when cooperation is based on long-standing trust and the number of participants is limited.

In the wake of the Snowden revelations, which revealed large-scale internet data monitoring and collection by the US and Western allies, many companies have reduced their level of information-sharing with the US government and distanced themselves from political partnerships that now appear toxic.[20] They have done this in an effort to salvage their reputation with current and potential international customers. International markets represents the majority of future growth potential for many US technology companies, and they cannot afford for their products to be compromised (or appear to be compromised).

Government limitations also extend to scale, people and buying power. For example, a large multinational manufacturing or defence company could easily have more (defensive) cyber security capability (in terms of people, process and technology) than many medium-sized countries. The people component is particularly crucial. Many governments struggle to attract and retain talented cyber security experts, and are forced to compete with the private sector for scarce talent. Few governments are capable of matching the US, which has the resources to supplement their cyber defence and intelligence agencies (such as the National Security Agency) with large and expensive contractor workforces.[21]

Government buying power in cyber security is also limited, relative to what they are accustomed to in traditional areas of security and defence. Militaries are the dominant buyers of submarines, warplanes and aircraft carriers, but for technology companies that sell hardware and software to a global market, even a government such as that of the US, Germany, or Japan is a minor player.

For example, the largest employer in the US is the Department of Defense with approximately 3.2 million civilian and military staff. But the Pentagon would have no hope making a bulk purchase and persuading Apple to produce an extra-secure version of the iPhone for all those employees. After all, in the final quarter of 2014, Apple sold approximately 65 million iPhones worldwide.[22] On occasion, governments can entice companies to produce specialised hardware or software, but this tends to be niche and highly expensive in the initial stages, with additional cost for upgrades and maintenance.

The international situation

> *The beautiful dream of the internet as a totally ungoverned space was just that—a beautiful dream. Like all utopian visions, it was flawed because it failed to account for the persistence of the worst aspects of human nature.*
>
> —Sir Iain Lobban, former Director of GCHQ[23]

The internet grew dramatically in the 1990s, propelled by the popularity of the web. This allowed online commerce to become commercially viable and cyber security rapidly became a topic of discussion. This happened particularly quickly in the US, which had a robust telecommunications network and had been developing precursors to the internet for several decades. Secure communications (enabled by encryption) had been the preserve of governments for decades, and only came to prominence in the private sector when online financial transactions (or 'e-commerce' as it was then called) were enabled by the growing popularity of the internet.[24]

In those early days the US controlled the basic protocols of the internet. Although some accommodation has been made since then, to account for the dramatic international growth of the internet, little has fundamentally changed. The US still retains a high level of influence over internet governance, even though the vast majority of internet users now reside outside of North America.[25]

Governance

Despite strong US influence, internet governance is gradually becoming more internationally representative. One example is the domain name system (DNS), which is the internet version of a telephone directory, and of which the US is slowly relinquishing control.[26] This has happened as governments around the world realise they need to become involved in discussions over the economic, social and political implications of internet connectivity. Global interest in the technical aspects of internet governance has also increased, largely due to the Snowden revelations, which demonstrated that US intelligence agencies has been using (and, in the opinion of many, abusing) the technological advantages enjoyed by the US.

Countries such as India and Brazil are becoming more assertive and there are a number of undecided 'swing states' that are yet to choose which governance model best fits their national interests—liberal, authoritarian, or something in the middle.[27] Russia and China are attempting to provide a counterweight to the political dominance over the internet of the US and Western Europe. However, their progress has been limited, and they have had difficulty gathering and maintaining international consensus and deciding on the most effective international body to use as a vehicle for their authoritarian vision of internet governance.[28]

High-level changes to the way the internet works (both governance and technical standards) take years to discuss, agree and implement, and are guided by economic and political priorities. There is more scope for action at the national level, for example with government filtering or censoring of internet traffic. In many cases these actions force users to provide their real names with email and social media accounts, sacrificing the freedom (through anonymity) that the internet has historically facilitated.[29] These actions are focused on imposing domestic control, but at the international level there is significant ambiguity regarding the actions of government.

Ambiguity and mistrust

It is extremely difficult to attribute online actions such as theft, disruption, espionage or sabotage to specific actors or groups with the same level of confidence that is possible in the physical world. There are many shades of grey in determining attribution, despite significant investments to do so by governments, companies, and security researchers.[30] This ambiguity presents opportunities for misdirection and misunderstanding, it has the potential to create and perpetuate mistrust, and complicates any attempts to codify international political agreements related to cyber security.

The current high levels of ambiguity in cyberspace (which is in the interests of many governments to maintain) mean that deterrence is a significant challenge. How can an attacker be deterred if their identity or affiliation is unknown? And what options does a government have if an adversary uses proxy actors such as individual hackers or organised criminals to launch attacks? When malicious software can be encrypted and transmitted online, or transported via a flash drive, what hope is there for traditional methods of monitoring and verification?

The Wassenaar Arrangement is one potential method for controlling the sale of software—such as surveillance packages or cyber attack tools—that is deemed to be dangerous in the wrong hands. The Arrangement is a voluntary, multilateral export control regime whose 41 member states exchange information on the transfer of arms and dual-use goods and technologies in an effort to improve national and international security and stability. In 2015, the US attempted to expand these export controls to include ‘intrusion software’, but the broad wording caused widespread concern in the cyber security and technology sectors, as it had the potential to encompass legitimate technologies and practices that are essential for robust cyber security.[31] Compared to export controls for missile technology and advanced materials processing, the control of software appears far more daunting and, in some instances, completely impractical.

The effects of digital disruption increase as a country becomes more connected, and this could plausibly create its own deterrent effect. For countries whose critical infrastructure is highly dependent on digital connections around the globe, the costs of mutual disruption may be sufficient to deter hostile action. This deterrent effect is more applicable at the government level, for policy-makers who have to consider the safety and stability of an entire country. Individual hackers and organised criminals have no such responsibilities and other incentives must be found to restrain their actions.

Attribution does not need to be iron-clad to formulate policy responses to undesired action. There are parallels with other areas of national security policy, such as the varying levels of attribution needed to take action related to arms trafficking or proliferation of weapons of mass destruction. If attribution can be improved through advanced technical means and supplemented by other intelligence and policy tools, then deterrence is not hopeless and there may even be the possibility of developing bi- or multilateral mechanisms that increase stability in cyberspace.

The development of cyber security treaties is still a long way in the future. Currently, there are high levels of mistrust—between the US and European democracies on one side, and Russia and China on the other side. From a national security perspective, there are limited incentives to cooperate or share sensitive information with nations that are not close allies.[32] It remains in the interest of many powerful states for power to be projected ambiguously in cyberspace, and it is almost inconceivable that they would restrain themselves through treaty obligations.

There is no international consensus (nor is there likely to be) on issues of national sovereignty such as intelligence gathering and surveillance of domestic populations. There is little agreement over the application of international law and what constitutes use of force in cyberspace, however the NATO-led publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* represents a significant though non-binding set of perspectives widely shared among NATO partners.[33] Neither Russia nor China have offered a similarly considered viewpoint of their own.

There is no adequate solution to these challenges and this has motivated governments to invest in the development of normative structures in the form of confidence building measures (CBMs), which can be designed for various purposes, for example:

- *Crisis management:* to establish lines of communication during or after an incident
- *Restraint:* to identify actors that have protected-status during conflict
- *Collaboration:* to bring actors together to adapt and apply existing norms;
- *Engagement:* to bring neutral actors together to establish new norms of behaviour and strengthen the stability of the internet.[34]

A series of international conferences—beginning in London in 2011—provided a high-profile forum to pull together major governments and companies to discuss CBMs and norms of behaviour in cyberspace.[35]

The international community, including the public and private sectors, has shown itself capable of cooperating on some common problems. The 2004 Budapest Convention on Cybercrime was a significant step forward in harmonising cyber crime laws and increasing international cooperation between law enforcement agencies on 'infringements of copyright, computer-related fraud, child pornography and violations of network security'.[36] However, both the development of CBMs and collaboration to address common problems tend to be incremental and long-term processes, disrupted regularly by geo-political disagreements and unresolved tensions. Progress is likely to be measured in decades.

Threat inflation

As the existential threat posed by nuclear conflict receded with the end of the Cold War, national security priorities—particularly in the West—have focused on more diffuse threats such as terrorism, the internationally destabilising effects of localised conflicts, and cyber security. These threats offer plenty of scope for rhetorical inflation or exaggeration by policy-makers or vendors in search of a sale, and cyber security is no exception.

A certain amount of hyperbole is evident in the stories of pending 'cyber catastrophe', and news headlines that equate defacement of websites with warfare, when in reality the defacement is equivalent to graffiti.[37] With minimal investigation, it often becomes evident that the messengers of doom have much to gain from focusing on worst-case scenarios or stereotyped adversaries. On occasion the evidence resembles a Cold War-style 'missile gap' that systematically overestimates the capabilities of adversaries.

Government evidence to support the likelihood of worst-case scenarios tends to be sparse and uninformative due to concerns around national security or intelligence 'sources and methods'. Evidence from cyber security and forensic companies can be slightly more useful but often doubles as a marketing campaign and should be closely scrutinised.

It is worth noting that the top policy positions in many governments—particularly security and defence—are filled by former cold warriors whose professional experiences and perspectives were shaped by the dominant conflict of the past 70 years. Cyber security is relatively new compared to most security and defence topics, and it is not always straightforward to understand where it is appropriate to draw parallels with past conflicts and where hyperbole is distorting the policy-making process. Analogies of nuclear deterrence, disarmament and non-proliferation are often used inappropriately, neither accounting for the unique technical challenges of cyber security nor the vast difference between nuclear holocaust and digital disruption.

Possible futures

When the building blocks of cyberspace are identified and their characteristics are understood, it is possible to look into the future and assess how this environment could evolve. While it is difficult to make predictions with any certainty, there are some useful indicators.

The number of connected users is growing steadily and is one primary indicator of digital growth. Between the early 1990s (when the web was launched) and 2015, nearly 40 per cent of the world's population has connected to the internet.[38] It is a certainty that, within the next generation, most of humanity will have access to the internet through a PC, mobile device, wearable computer, or something yet to be conceived. And it is not just people communicating across the internet, it is also devices communicating with each other and with people. These devices will increase exponentially and by 2020 there will be an estimated 50-75 billion devices connected to the internet.[39] The data generated by these devices will help us to better understand our world but will also have to be carefully managed and secured.

Commercial trends will continue to shape the digital world as advances are made in connectivity, speed and storage. Computing power will continue to increase steadily, providing new opportunities for all actors, whether malicious and benign. Miniaturisation will allow smartphones and other computing devices to be packed with more sensors that interact with their environment and generate vast quantities of data.

Cyber security will grow in importance as dependence grows on a digital environment that is now essential to much of the world's population. It will be possible to connect nearly anything to the internet, and to use software to replace mechanical processes (such as in cars or factories).

Risk management will be more difficult for both the public and private sectors, given increasing levels of interconnection and complexity that conceals risks. When disruption occurs—either intentional or accidental—it will produce cascading effects that ripple through other sectors, with second and third-order consequences that will be nearly impossible to predict. Given such a high level of uncertainty, resilience will become more important and investments will be made in significantly strengthening the governance and technical foundations of the internet.

The majority of major technology companies have emerged from the West, although this is rapidly changing as Chinese technology, online commerce, and smartphone companies are expanding abroad and providing genuine competition for the incumbents. The motivation to expand internationally will result in increased tensions, as governments force domestic companies to share (internationally-gathered) information for law enforcement or national security purposes.

This dilemma has persisted in the US and UK for some time. It will be replicated in China, where domestic companies with international ambitions and significant resources will find themselves at odds with the national security priorities of an increasingly assertive Beijing. Customer pressure will factor into this as well. Multinational technology companies (such as Facebook, Google, and Alibaba) will be caught between law enforcement demands from countries where they do business, and the growing desire of users for more privacy and control of personal data.

Following the Snowden revelations, the loss of trust between the US Government and US-based technology companies will continue. This is one indicator of the espionage-related international tensions that will increase as governments around the world invest in a variety of capabilities related to digital offence and defence. Internet governance will be hard-pressed to stabilise this environment and, if the last decade is indicative of the next one, progress will be limited to gradually establishing norms, codes of conduct, and CBMs.

Conclusion

Security problems have inevitably arisen as the internet became the central nervous system of the globe, but these challenges must be viewed in the context of all positive changes that have emerged. The internet has empowered individuals around the globe, unleashed unprecedented levels of innovation and creativity, and created new markets while disrupting old ones. This capacity for disruption is a 'feature, not a bug, i.e. an intentional facility, not a mistake' in the design of the internet, and it benefits all users.[40]

Attention on cyber security will continue to grow as dependence on digital networks increases. These are risks that must be managed, not exaggerated. One sign of a mature digital environment will be when these risks are managed in the same way as other economic, social, and political risks that humanity has adapted to over the centuries. That maturity is a long way off, and between now and then there is still much work to be done harnessing the opportunities of cyberspace while understanding and minimising the dangers.

The views and opinions expressed are the author's own, as are any inaccuracies in fact or interpretation.

Endnotes

1 The term 'cyberspace' was first coined by science fiction author William Gibson in his 1984 book *Neuromancer*, where it was also defined as 'a consensual hallucination experienced daily by billions of legitimate operators'. TechTerms, 'Cyberspace', www.techterms.com/definition/cyberspace

2 UK Cabinet Office, 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world', *UK Government*, November 2011, www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, pg. 11. An overview of varying national definitions of cyberspace can be found in D. Rajnovic, 'Cyberspace – What is it?', *Cisco*, 26 July 2012, blogs.cisco.com/security/cyberspace-what-is-it/

3 web.mit.edu/ecir/pdf/clark-cyberspace.pdf

4 TechTerms, 'Internet', www.techterms.com/definition/internet

5 In the 1990s this was known by its full name, the World Wide Web, hence the 'www' at the front of every web address. TechTerms, 'www', www.techterms.com/definition/www

6 J. Naughton, 'The internet: Everything you ever need to know', *The Guardian*, 20 June 2010, www.theguardian.com/technology/2010/jun/20/internet-everything-need-to-know, C. Anderson and W Wolff, 'The Web Is Dead. Long Live the Internet', *Wired*, 17 August 2010, www.wired.com/2010/08/ff_webrip/all/

7 G. Dallas, 'Making sense of Internet Platforms: Network Effects and Two Sided Markets', *George Dallas*, 5 June 2014, georgemdallas.wordpress.com/2014/06/05/making-sense-of-internet-platforms-network-effects-and-two-sided-markets/

8 S. Kessler, 'Twitter Can Track Disease — Can It Predict Outbreaks?', *Mashable UK*, 8 June 2012, mashable.com/2012/06/08/social-media-disease-tracking/

9 TechTerms, 'Botnet', www.techterms.com/definition/botnet

10 W. Isaacson, 'Inventing the Future, 'The Idea Factory', by Jon Gertner', *The New York Times*, 6 April 2012, www.nytimes.com/2012/04/08/books/review/the-idea-factory-by-jon-gertner.html?pagewanted=all

11 S. Shankland, 'Moore's Law: The rule that really matters in tech', *CNET*, 15 October 2012, www.cnet.com/news/moores-law-the-rule-that-really-matters-in-tech/

12 J. Lewis (@james_a_lewis), 'Rethinking digital development (effect of internet is to lower transaction costs; everything else is advertising). What's missing?', *Twitter*, 9 January 2012, 1:36pm, twitter.com/#!/james_a_lewis/statuses/156368736209747969

13 C. Doctorow, 'Lockdown: The coming war on general-purpose computing', *boingboing*, December 2011, boingboing.net/2012/01/10/lockdown.html

14 C. Doctorow, 'Lockdown: The coming war on general-purpose computing', *boingboing*, December 2011, boingboing.net/2012/01/10/lockdown.html

15 BBC News, 'Cows connected to web to boost milk', *BBC*, 24 March 2014, www.bbc.co.uk/news/uk-scotland-scotland-business-26705812

16 Q. Norton, 'Everything Is Broken', *Medium*, 20 May 2014, medium.com/message/everything-is-broken-81e5f33a24e1

17 B. Krebs, 'The Scrap Value of a Hacked PC, Revisited', *Krebs on Security*, 15 October 2012, krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

18 J. Glanz and J. Markoff, 'Egypt Leaders Found 'Off' Switch for Internet', *The New York Times*, 15 February 2011, www.nytimes.com/2011/02/16/technology/16internet.html?_r=2&hp=&pagewanted=all&

19 C. Matlack, 'Swift Justice: One Way to Make Putin Howl', *Bloomberg Business*, 4 September 2014, www.bloomberg.com/bw/articles/2014-09-04/ultimate-sanction-barring-russian-banks-from-swift-money-system

20 D. Sanger and N. Perlroth, 'Obama Heads to Tech Security Talks Amid Tensions', *The New York Times*, 12 February 2015, www.nytimes.com/2015/02/13/business/obama-heads-to-security-talks-amid-tensions.html?_r=0

21 A. Bloomfield, 'Booz Allen Hamilton: 70% of the U.S. Intelligence Budget Goes to Private Contractors', *Policy.Mic*, 14 June 2013, www.mic.com/articles/48845/booz-allen-hamilton-70-of-the-u-s-intelligence-budget-goes-to-private-contractors

22 L. Whitney, 'China likely to top US for Apple iPhone sales', *CNET*, 26 January 2015, www.cnet.com/uk/news/china-likely-to-top-us-for-apple-iphone-sales/

23 I. Lobban, 'Sir Iain Lobban's valedictory speech – as delivered', *GCHQ*, 21 October 2014, www.gchq.gov.uk/press_and_media/speeches/Pages/Iain-Lobban-valedictory-speech-as-delivered.aspx

24 H. Abelson, K. Ledeen, and H. Lewis, 'Secret Bits: How Codes Became Unbreakable', *informIT*, 3 June 2008, www.informit.com/articles/article.aspx?p=1218422&seqNum=5

25 Asia has nearly 1.4 billion users, or approximately 45% of the global total. Internet World Stats, 'Internet Users in the World: Distributed by World Regions – 2014 Q2', *Miniwatts Marketing Group*, 30 June 2014, www.internetworldstats.com/stats.htm

26 C. Farivar, 'In sudden announcement, US to give up control of DNS root zone', *arstechnica*, 15 March 2014, arstechnica.com/tech-policy/2014/03/in-sudden-announcement-us-to-give-up-control-of-dns-root-zone/

27 D. Clemente, 'Adaptive Internet Governance: Persuading the Swing States', *The Centre for International Governance Innovation*, October 2013, www.cigionline.org/sites/default/files/no5_3.pdf, T. Maurer and R. Morgus, 'Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate', *The Centre for International Governance Innovation*, May 2014, www.cigionline.org/sites/default/files/no7_2.pdf

28 K. McCarthy, 'China and Russia start again with this UN internet takeover bull****', *The Register*, 4 February 2015, www.theregister.co.uk/2015/02/04/un_china_russia_internet/

29 P. Carsten, 'China to ban online impersonation accounts, enforce real-name registration', *Reuters*, 4 February 2015, www.reuters.com/article/2015/02/04/us-china-internet-censorship-idUSKBN0L80ZF20150204

30 T. Rid and B. Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 2015, 38:1-2, 4-37, www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382

31 Sean B. Hoar and Bryan Thompson, 'Pardon the 'Intrusion' – Cybersecurity Worries Scuttle Wassenaar Changes', Davis Wright Tremaine LLP – Privacy and Security Law Blog, 4 September 2015, www.privsecblog.com/2015/09/articles/cyber-national-security/pardon-the-intrusion-cybersecurity-worries-scuttle-wassenaar-changes/

32 The decades-long 'Five Eyes' agreement among the Anglophone countries (the US, UK, Canada, Australia and New Zealand) is the most prominent example of an enduring signals intelligence relationship. P. Farrell, 'History of 5-Eyes – explainer', *The Guardian*, 2 December 2013, www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer

33 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'Tallinn Manual', ccdcoe.org/research.html

34 Atlantic Council, 'Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security', *NATO Advanced Research Workshop on Confidence-Building Measures in Cyberspace*,

5 November 2014, www.atlanticcouncil.org/publications/reports/confidence-building-measures-in-cyberspace-a-multistakeholder-approach-for-stability-and-security

35 About the Global Conference on CyberSpace 2015, www.gccs2015.com/gccs/all-about-gccs2015

36 Council of Europe Treaty Office, 'Convention on Cybercrime', *Council of Europe*, 1 July 2004, conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185

37 Xkcd, 'CIA', xkcd.com/932/

38 World Wide Web Foundation, 'History of the Web', webfoundation.org/about/vision/history-of-the-web/

39 T. Danova, 'Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020', *Business Insider*, 2 October 2013, www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10?IR=T

40 J. Naughton, 'The internet: everything you ever need to know', *The Observer*, 20 June 2010, www.guardian.co.uk/technology/2010/jun/20/internet-everything-need-to-know