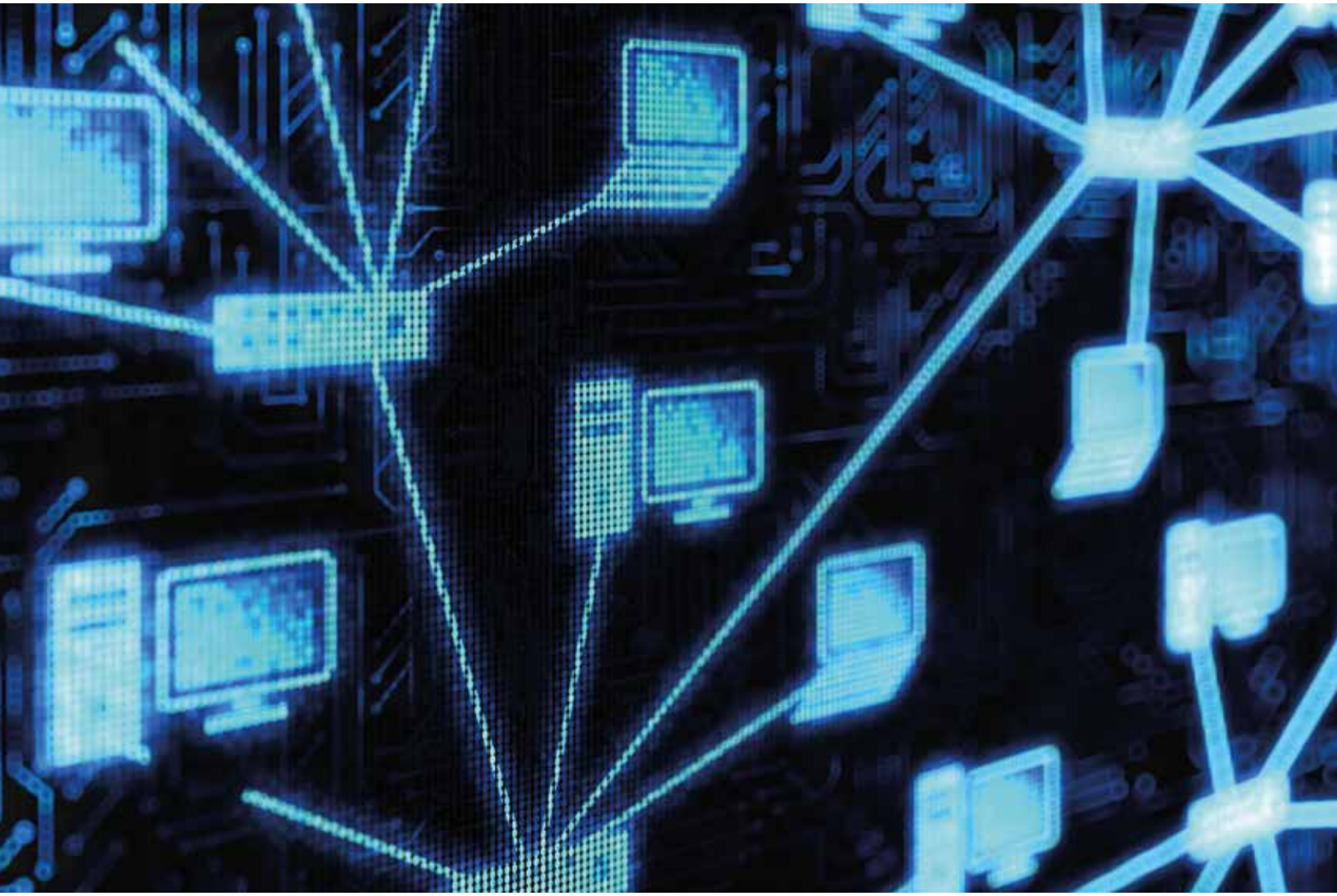
HIERARCHY OF CYBERSECURITY NEEDS

Developing national priorities in a connected world



Oxford Analytica

Commissioned by
Microsoft Trustworthy Computing

Microsoft

Table of contents

About this report

Commissioned by Microsoft Trustworthy Computing

November 2013

Oxford Analytica is a global analysis and advisory firm which draws on a worldwide network of experts to advise its clients on their strategy and performance. Our insights and judgements on global issues enable our clients to succeed in complex markets where the nexus of politics and economics, state and business is critical. To learn more about our products and services, visit **www.oxan.com**

HEAD OFFICE
5 Alfred Street, Oxford OX1 4EH
T +44 1865 261 600

USA
1069 Thomas Jefferson Street, NW
Washington DC 20007
T +1 202 342 2860

405 Lexington Avenue, Suite 54B, New York, NY 10174
T +1 646 430 9014

FRANCE
5, Rue de Surène, 75008 Paris
T +33 1 42 89 08 36

www.oxan.com

Introduction

The state has traditionally assumed responsibility for national security, citizen welfare, economic growth, public health and a range of aspects that are fundamental to the prosperity and well-being of a country. The internet has become such a pervasive part of public and private life that it is now a vital component in almost all of these areas of state responsibility.

In response, governments are developing cyber strategies, policies and plans to address the enormous benefits and associated risks that come with the rise of internet connectivity. Central to these national efforts is the need for cybersecurity. But what are the responsibilities of the modern state in providing cybersecurity for individuals, organizations and its own operations? How can governments think about using cybersecurity to help enable their country to benefit from the full potential of the internet?

Abraham Maslow's Hierarchy of Needs offers a way of structuring the answer to these questions. Maslow's hierarchy takes a step-by-step approach to describing human motivation, outlining an ascending set of needs that represent an individual's most basic requirements (food, water) and build towards more aspirational goals, in line with conceptions of well-being. Once an individual satisfies all the needs in the hierarchy, that individual is considered to have reached their full potential.

This report explores the application of Maslow's hierarchy to the internet, articulating the ascending stages towards full exploitation of the internet's potential while considering cybersecurity at every level. Understanding the cybersecurity hierarchy of needs at a national level allows governments to take advantage of growing opportunities for the internet-enabled economy while improving risk management for existing and future cybersecurity threats. Through this lens, governments can think about their own nation's status within the hierarchy and prioritize the appropriate security measures to improve their ability to create an environment where citizens, enterprises and the state itself can realize the internet's full potential to help people and businesses.

The internet is a shared domain and the conversation about cybersecurity must include a broad set of stakeholders. Neither governments nor the private sector acting in isolation can fully respond to the security implications of the scope and pace of change occurring on the internet. Bearing this broader conversation in mind, this report focuses more narrowly to address state actors and their responsibilities to the individuals and enterprises within their borders, as well as setting priorities across national boundaries.

HIERARCHY OF CYBERSECURITY NEEDS

Modern ideas about how governments provide security and well-being for their citizens and domestic enterprises have evolved over centuries, historically marked by the Westphalian concepts of sovereignty of nation-states. Conceptions of citizen protection from the state have similarly evolved, including the rule of law, due process, habeas corpus and other governance norms. Modern societies are now faced with the challenge of quickly applying traditional and well-evolved governance concepts to cybersecurity in ways that make sense for a digital world. This challenge has become even more pointed with recent debates over the appropriate role of government in overseeing our online data.

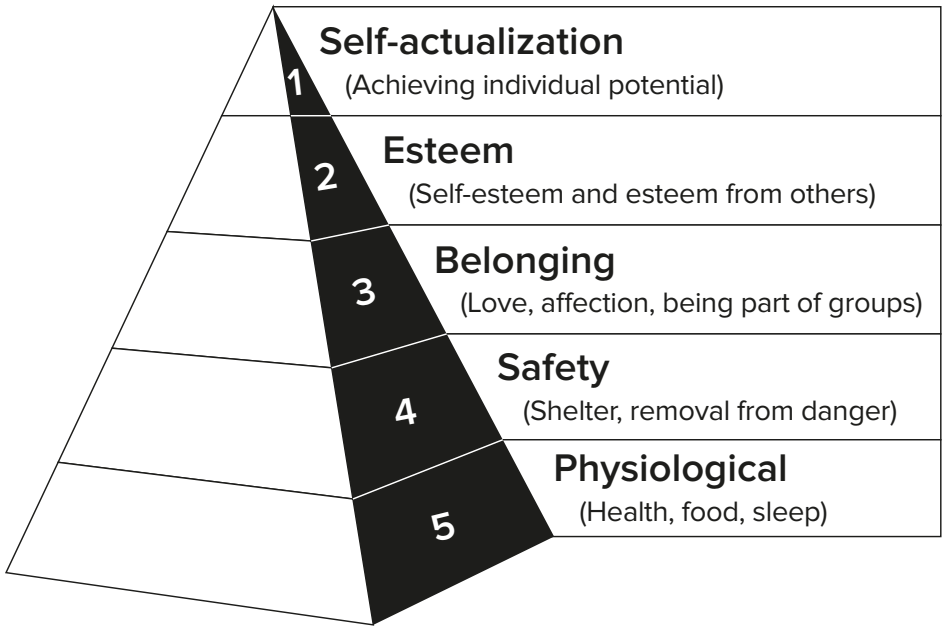
To think about this challenge, we can conceive of a Hierarchy of Cybersecurity Needs that separates out the dimensions of ascending needs (or goals) of internet users that governments have a role in securing. Once these needs are met, they ultimately enable the optimum operating state of the internet, where individuals and enterprises can reach *their* full potential by exploiting *the internet's* full potential.

The cybersecurity concept of needs builds on Abraham Maslow's Hierarchy of Needs (see Figure 1), first outlined in 1943.[1] Maslow identified five types of needs: physiological, safety, belonging, self-esteem and self-actualization. He arranged these needs hierarchically, and argued that when lower needs are unsatisfied, they dominate motivation and behaviour, but once they are satisfied higher needs emerge.

The lower levels of Maslow's hierarchy consist of the most basic and physical needs, like food, water and sleep. Once these needs are met, people look to satisfy the next tier of needs, which are increasingly complex and sophisticated as they move to the top of the pyramid. These include safety, then a feeling of belonging within a group, followed by the need to feel self-esteem or to be esteemed by others. These needs are in sequence: an individual will be primarily focused on meeting one tier of needs before moving on to the next. Once an individual has met all the needs in the pyramid, they are deemed to have reached their full individual potential.

1 Maslow, A.H., 'A theory of human motivation'. Psychological Review, 50(4), 1943, pp 370--396

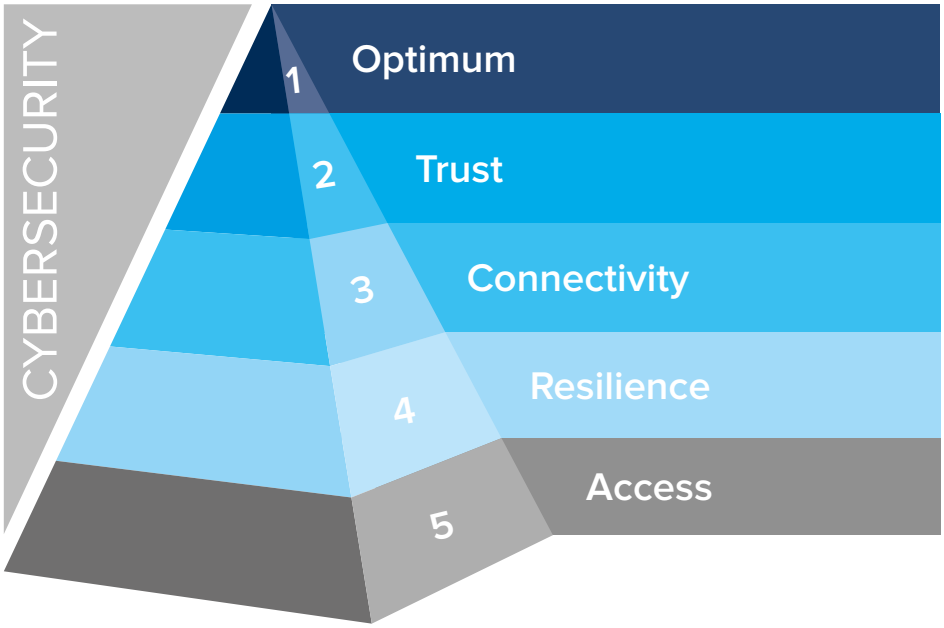
Figure 1: Maslow's original hierarchy of needs



Maslow's hierarchy depicts an ascending set of needs that individuals pursue in sequence, eventually reaching self-actualization where they achieve their full individual potential.

We have adapted the hierarchy of needs concept to explore cybersecurity: defining the needs of individuals, enterprises and governments as they progress through the stages of internet engagement in pursuit of full exploitation of the internet's potential. At each tier, a user is engaging with the internet in a different way and with varying impact. And at each tier, cybersecurity has a role to play, one which starts at a relatively low base when we discuss basic access and then grows in complexity and importance as we expect the internet to remain resilient while supporting our critical infrastructure, to connect us with fundamental services, and ultimately, to be trustworthy as we increasingly incorporate information and communications technology (ICT) systems into our daily lives.

Figure 2: Hierarchy of Cybersecurity Needs



The Hierarchy of Cybersecurity Needs separates out the dimensions of ascending needs (or goals) of internet users that governments have a role in securing. Meeting these needs enables the optimum operating state of the internet, where individuals and enterprises can reach their full potential by exploiting the internet's full potential.

We have envisioned these needs as follows:[2]

- The first need, or goal, is simply to have **access** to the internet.
- Secondly, a user needs the internet to be **resilient** -- available reliably and predictably.
- Following that, the user seeks to engage with others in an increasingly interconnected and substantive way: **connectivity.**
- Then, the user needs to have full **trust** that their use of the internet is secure enough for their intended purpose. Having only partial trust in the internet will limit what information users are willing to share or which services they are willing to conduct online.
- Once these needs are cumulatively met, the user is able to exploit the internet's **optimum** state without constraint. The internet can then become fully actualized, as Maslow's individual is when he/she satisfies their cumulative set of needs. In other words, the internet's potential to help people and businesses is fully realized.

2 The precise order of the tiers can certainly be debated: for instance, many people will gain access and achieve connectivity while lacking resilience and facing patchy communications, and innovations in connectivity can outpace resilient infrastructures. However, we have proposed a sequence in this pyramid that is most relevant from the perspective of a policymaker or other government actor in determining priorities.

Our categories here can be loosely mapped to Maslow's:

- physiological needs to access;
- safety to resilience;
- love and belonging to connectivity;
- esteem to trust; and
- the experience of self-actualization to the optimum.

The needs play out in much the same way as Maslow's hierarchy. A person who cannot yet access the internet is not concerned with how resilient it is. Similarly, a user who cannot rely on the dependable availability of the internet may not yet be preoccupied by the degree to which they may be able to trust their data on it.

Take the example of an individual considering opening an online banking account. They will first need access to the internet to even consider this as an option. When that need is satisfied, they will then have to be assured that they can have reliable access to the internet so that it can be useful to them on a consistent basis. Their main focus will be whether they would be able to view their balance when they need to, and transfer money or make payments when they want to. If a user has access that is reliable, he/she will then need to be able to connect with the banking institutions online, ideally amongst a critical mass of reputable banks competing for their online business. Finally, before someone moves their personal banking operations fully online, they will have to trust the network. It is only when all these needs are cumulatively met that the user can realize the full potential of the internet in online banking services: convenience, flexibility and resource efficiency.

There are important cybersecurity considerations at each point in this layered set of needs, represented by the lefthand triangle that expands as the needs ascend. The hierarchy of cybersecurity needs suggests that cybersecurity plays a key role in the ability of countries, businesses and individuals to fully harness the internet's potential to improve their governance, operations and lives.

This report

This report discusses the needs of an internet user at each level and the role of cybersecurity in meeting that need. Every section includes a case study that explores the development or response to this need in the real world. Finally, the report outlines recommendations for government-led cybersecurity priorities at each level.

SECURITY AND UTILITY

In discussing the importance of cybersecurity, we must also address the trade-offs between the needs outlined in the hierarchy and cybersecurity itself. In more basic terms, the problem involves a tension between **the security** and **the utility** of a computer system or network. A completely secure computer or network is one with no connections to external sources, but this renders it almost futile for most modern applications. Yet as the number of access points in a society increases, so do the vectors for an opportunistic attacker to travel. Expansion of access multiplies the number of potential vulnerabilities (no matter how small these vulnerabilities might be individually). Therefore neither absolute safety nor absolute convenience is attainable or desirable.

By using the tiered hierarchy model to consider the relationship between security and utility, rather than assuming they are in a single, zero-sum relationship, this report seeks to show that a holistic and balanced approach to security can not only increase utility but help users reach a whole new level of engagement with the internet for personal and organizational development. Far from being a brake on creativity and interaction, cybersecurity can be an enabler of innovation and shared experience.

Access: The Basics

The first essential need for an individual to gain benefits from the internet is simply access to it. The term 'access' can carry a range of meanings and involve questions of location, speed, cost and security -- these are all essential components of the access issue.

Access to the internet has spread more quickly than any other preceding communications technology. While it took radio more than 75 years to reach an audience of 50 million, and television needed 13 years, the internet reached the same number of users in only four years.[3] It is a serious challenge for cybersecurity and governance to keep up with this pace and scale.

Meeting the need for access

At this level, individuals seek access to the internet, and the government can play an instrumental role in providing it. There are three main types of limitations that governments can target to expand access for their citizens:

- **Structural,** which may be due to lower levels of economic development, insufficient ICT infrastructure and/or low consumer priority for expenditure on communications;
- **Political,** where internet providers, content-generators and users may face institutional pressure to comply with domestic policies in ways that clash with internationally recognized human rights like freedom of expression and privacy; and
- **Affordability.** According to current ITU estimates, the price of an entry-level mobile-broadband plan represents between 1-2% of monthly gross national income per capita in developed countries whereas it represents 11-24% in developing countries.[4] The gap is even more extreme in prices for fixed-broadband, with developed countries experiencing a virtuous circle in which falling prices increase penetration, thereby exerting further downward pressure on pricing. But that has yet to happen in countries where access through mobile phones is often the first form of internet access available.

We can also consider social barriers to access, where the use of technology is limited for certain groups, for instance women or marginalized social groups.

3 United Nations, 'We the Peoples: The Role of the United Nations in the 21st Century", March 2000, p 32
4 International Telecommunication Union, "The World in 2013: ICT Facts and Figures", 2013

By most metrics, however, access has greatly improved in the last ten years (see Figure 3). As of 2012, almost one-third of the global population had used the internet.[5] Over 30% of people in the developing world are online, and more than 75% of the developed world. There are still discrepancies within those broad categories; for example, the percentage of those online in Africa is only half the number of the Asia Pacific region, yet the year-on-year growth rate for mobile broadband in Africa is almost twice that of Asia Pacific.

Access increases cybersecurity needs

Education and awareness campaigns may be just as effective as technical security responses in addressing basic access level risks

In areas that have recently gained access to the internet, the need for cybersecurity measures is clear but perhaps less complicated than at higher levels of the pyramid. Users are new to the internet and learning to navigate the digital environment. This presents challenges to governments that are related to legislative, technical and educational aspects.

Technology often advances more quickly than governments can create legislation and regulation to account for it. For countries that are undergoing a rapid expansion in internet access, a communications policy framework will be crucial in shaping the security environment. This framework can include laws, norms and values around cybersecurity. Governments can work with peers or advisors to implement known best practices or establish tailor-made policy for their national context. At the same time, the current international cybersecurity policy framework is fragmented and more competitive than cooperative. Therefore, governments at the 'access' level of the hierarchy will have to carefully consider their own security policies and where they fit into the international policy spectrum.

More citizen-level action will also be required. Communities that have only recently gained access to the internet may be more susceptible to social engineering attacks, whereby seemingly legitimate emails deliver malicious code or convince recipients to give up information or to click on a malicious link. Encryption, effective password policies and least-privilege accounts can be instituted or required by organizations to minimize the risk of social engineering with minimal disruption. Similarly, encouraging users to maintain device hygiene is very important; keeping devices patched, using antivirus and regular scanning for malware can help meet cybersecurity needs at this level. Finally, education and awareness campaigns may be just as effective as technical security responses in addressing basic access level risks. Over 50% of compromises still involve social engineering,[6] so awareness campaigns can significantly reduce the potential for cybercrime.

The following case studies focus on countries and regions that saw their access to the internet rapidly expand in a short period of time and the role of their governments in enabling and protecting the needs of users at the first level of the hierarchy.

THE RIGHT TO INTERNET ACCESS

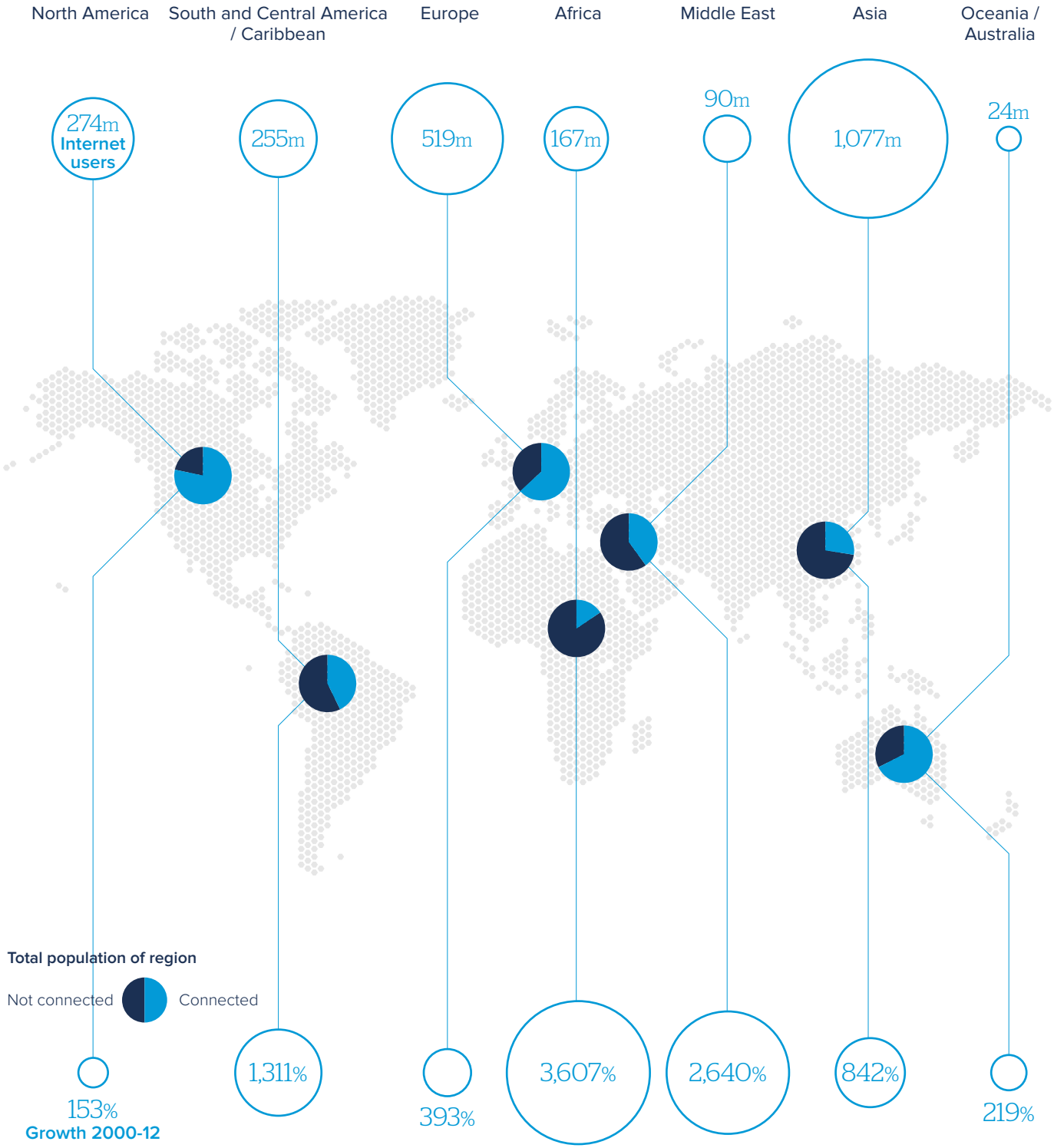
Many countries today pursue policies seeking to bolster the availability and speed of broadband services. Some of this policy action is driven by the idea that internet access is a basic human right -- or at the least a civil right -- which echoes earlier debates about widespread access to telephone services. Further, the treatment of internet access as a right has reopened the conversation on the government's role in communication infrastructure from both a regulatory, investment and operational standpoint.

Uneven access is also concern, which manifests as a "digital divide" that exacerbates existing socio-economic gaps. In other words, the expansion of access alone does not resolve the need; it merely alters the nature of the problem, with different users able to use the internet to different degrees of usefulness.

5 World Economic Forum, Global Agenda Council on the Future of the Internet 2012-2013
6 Charney, S., Microsoft, 'Trustworthy Computing Next', 2012

Figure 3: Growth of internet by region, 2000-12

The connected world: internet use by region, 2000-12



Source data from Miniwatts Marketing Group, 2012.

CASE STUDY: IMPACT OF FIBER-OPTIC ACCESS FOR EAST AFRICA

East Africa, and Kenya in particular, experienced a rapid spread of access to the internet following the arrival of fiber-optic cables in 2009. As Kenyan citizens were able to overcome the structural limitations to access and subscription became more affordable, internet penetration skyrocketed. At the same time, however, so did the number of potential targets for an opportunistic attacker to reach. The government had to consider policies that would both create an enabling environment for the budding information communications sector and protect the drastically expanding user group from cybercrime at an individual and commercial level. It also began to consider which of its own functions it could reasonably and safely move online. The priorities were to craft legislative infrastructure for communications security and promote user awareness of cyber threats.

Broadband comes to East Africa

Before 2009, East Africa was the last major region on Earth without fiber-optic broadband internet access. The sub-Saharan African region -- one of the poorest in the world -- was paying some of the highest prices in the world for internet access. Due to a lack of basic infrastructure, eastern and southern Africa saw bandwidth prices as high as 40 times those in the United States, since Africa was reliant on expensive and slow satellite connections for access.[7] Less than five years ago, many countries in the region, including Kenya, could only access broadband through satellite. Although 8 million Kenyans -- approximately 20% of the population -- were connected to mobile internet services, the provision of high-speed internet access within the country was not widespread.

In July 2009, the SEACOM submarine fiber-optic cable network system was launched, directly connecting South Africa and East Africa with Europe and Southern Asia. The cable drastically increased the availability and lowered the cost of broadband services in East Africa. The SEACOM cable (along with others like EASSY and TEAMS that landed shortly after SEACOM) contributed significantly to Africa's extraordinarily high mobile broadband growth rate, which has averaged 82% year-on-year between 2010 and 2013.[8] On the country level, Kenya has seen exponential growth in the number of broadband subscribers over

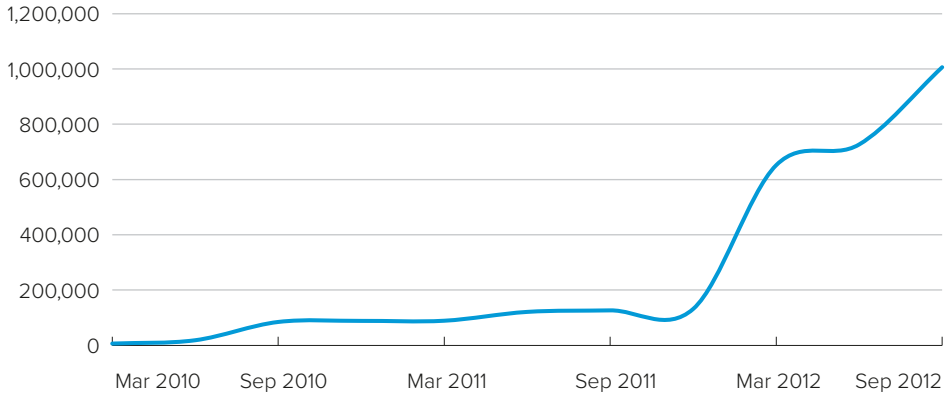
7 Private Infrastructure Development Group
8 International Telecommunication Union, "The World in 2013: ICT Facts and Figures", 2013

the last three years, with a seven-fold increase in 2012 alone (see Figure 4). Given that the current subscriber base -- 1 million as of end-2012 -- constitutes just 2.5% of the country's total population, expectations of a continued dramatic level of growth are high.

Enabling and protecting the new ICT sector

With access to the internet rising, the Kenyan government placed added focus on reaping the benefits that access can provide. Research has found that investment in the information and communications technology (ICT) sector, and specifically an increase in the ICT penetration rate, can have a positive effect on economic growth through three primary channels: increased innovation; increased information (resulting in better decision-making by companies and individuals); and an increase in output levels.[9]

Figure 4: Skyrocketing access in Kenya (total broadband subscribers in Kenya, 2010-2012)



Source data from the Communications Commission of Kenya

Accordingly, the Kenyan government's 2009 national development plan, Vision 2030, targeted the IT-enabled service industry as one of its six pillars of economic growth over the next two decades. This plan explicitly recognizes that Kenya's future socio-economic development will increasingly depend on the ability of its citizens to use ICT innovations as tools and enablers of production, and sets out the policy structures to support the sector. The government also introduced the Tandaa Digital Content Grant, an 88 million dollar scheme funded through the World Bank, which seeks to promote the development of local digital content. The Information and Communication Permanent Secretary, Bitange Ndemo, noted: "We have moved from discussing infrastructure to policy, content and capacity-building in the industry."[10]

Though the government's ambitious goals for IT-led growth have not all been met, the spread of internet access has been credited with the progress of the Kenya's smaller, high-tech startup companies specializing in software development and IT consulting, and a general shift from local firms focusing on exports to those that focus on the local market.[11,12]

9 Vu, K. M., 'ICT as a source of economic growth in the information age: Empirical evidence from the 1996--2005 period', Telecommunications Policy, Vol. 35, No. 4, 2011, pp 357-372

10 Kenya ICT Board. 'ICT Innovators get a boost of over a 100 million from Government', quoted in Graham, M., Mann, L., 'Imagining a Silicon Valley: Technological and Conceptual Connectivity in Kenya's BPO and Software Development Sectors.' The Electronic Journal of Information Systems in Developing Countries 56 (2), 2013, pp 1-19

11 Graham, M., Mann, L., 'An Import or an Export? The Transnationalization of Labour Practices in Kenya's Business Process Outsourcing Sector.' Conference paper presented at ECAS 2013

12 Ibid.

The role of cybersecurity

Despite the clear benefits the cables have provided, certain challenges have become apparent in the four years since their installation. Cybercrime has been on the rise, and the government has had to rapidly create the political and legal reforms to adapt to its new internet presence, for example amending its Communications Act to better account for electronic transactions and creating a Cyber Security and Data Protection Bill.

The ICT sector still faces a number of challenges. The 2012 progress report from Kenya's Ministry of Planning, National Development and Vision 2030 cited poor cybersecurity as one of the key impediments to the growth of the sector in the medium term.[13] More recently, Kenya has launched a national cybersecurity strategy, as part of an ICT master plan that is designed to guide the government and private sector from a reactive to a proactive approach to cybersecurity issues.

MICROSOFT 4AFRIKA

Microsoft's continent-wide 4Afrika initiative* is a 75 million US dollar project that aims to bring one million African small businesses online over the next three years. In Kenya specifically, its Mawingu project is providing low-cost, high-speed broadband for rural areas in partnership with both the government and Indigo, a local internet service provider. Other programs affiliated to Microsoft 4Afrika address similar access shortfalls across the continent. In partnership with Huawei, Microsoft developed the Windows Phone 4Afrika, a smartphone specifically designed for quality and affordability, and equipped with custom applications designed by local African developers for Africa. Microsoft has also launched an education platform that offers training to potential web developers aimed at improving their employability within African economies.

Initiatives such as 4Afrika can help to provide initial access to the internet, but also to enhance the country's cybersecurity infrastructure. In this area, companies with technology and cybersecurity experience can bring their expertise to an environment where current security measures are still being developed and understood.

* www.microsoft.com/africa/4afrika

13 Kenya's Ministry of State for Planning, National Development and Vision 2020, 'Third Annual Progress Report', 2010-2011, p 49

CASE STUDY: ESTONIA'S IT REVOLUTION

Estonia's internet access rose significantly from a low base at the time it gained independence in 1991 to today, where the internet is so deeply embedded in daily life that the country has been dubbed "e-Stonia". The experience of Estonia's embrace of information technologies provides insights on core problems of cybersecurity, demonstrating both the benefits and challenges of rapid access to the internet in modern societies.

Estonia shows the potential of the swift expansion of internet access to 'leapfrog' other nations on the development path; by implementing near-total internet access, the government unlocked efficiencies and gained enormous economic and social benefits. It also suffered a cyberattack in 2007 that debilitated financial and government activity in the country for a few weeks. Instead of prompting a rollback from pervasive internet access, this was an impetus for the government to further bolster cybersecurity. For instance, the government's implementation of card-based authentication has provided a robust layer of protection for access to financial and government services, from tax filing to voting and health services.

e-Stonia

Nowhere, perhaps, is the internet so ubiquitous in public and private life as in Estonia. Since 2000 access to the internet has been written into domestic law as a fundamental human right. In 2007 Estonians became the first citizens in the world to cast parliamentary votes online; one-quarter of ballots in the last election, held in 2011, were electronic. Cabinet sessions are paperless and employ a web-based portal. Ninety-eight percent of financial transactions and 94% of tax filings are performed online. Every school is connected to the internet. A new business can be registered online without any bureaucratic hindrance; the process takes 18 minutes. The country, in brief, has earned its moniker of "e-Stonia."

Access as a transitional strategy

Estonia's internet revolution is often regarded as something of a miracle. There is good reason for that: the explosion in digital access followed the country's return to independence in 1991 as it emerged out of conditions created by five decades of Soviet central planning.

The Estonian IT transition was conceived and orchestrated -- initially -- by the government. It resulted from a concerted commitment by decisionmakers to what has been termed the "third wave" theory of economic development: the idea that a transitional society can attain prosperity swiftly by linking citizens and the state together through means of instantaneous

Estonia's leaders saw internet access as a vehicle for economic ascendancy over already developed nations, allowing Estonia to leapfrog past them

communication. Estonia's leaders also saw internet access as a vehicle for economic ascendancy over already developed nations, allowing Estonia to leapfrog past them. As former Prime Minister Mart Laar said: "[C]ountries which use high technology and modern means of communication in order to increase development gain control over the 'second wave' countries coming from the industrial society."

This vision acquired formal expression in 1994 with the drafting of the government's first "information society" strategy. Two years later, then-foreign minister (and now president) Toomas H. Ilves proposed the "Tiger Leap" (Tiigrihüpe) project, aiming to provide internet access to all Estonian schools. Structural factors, most notably technology transfers and capital inflows from nearby Nordic countries, gave further impetus to the development of a native IT base.

Estonia has reaped enormous economic and social benefits from the rapid growth in access after 1991 (though it is worth noting that Estonia's population is only 1.3 million). The country has become a center of high-tech excellence in Europe, giving rise to such lucrative innovative ventures as Skype. The national electronic ID card system, which supports a multitude of citizen e-services, such as online voting and banking, binds the state and citizen in a close relationship that would have seemed impossible only a generation ago. Pervasive internet access has been the centerpiece of Estonia's successful adoption of democratic reforms; the country's transitional success is inconceivable without it.

Access and security in Estonia: a mixed relationship

Yet Estonia's leap into the information revolution came with drawbacks. The country has had to face the consequences of its success -- namely, increased vulnerability to cyberattack.

A 2007 attack intermittently paralysed financial and government activity for a period of a few weeks

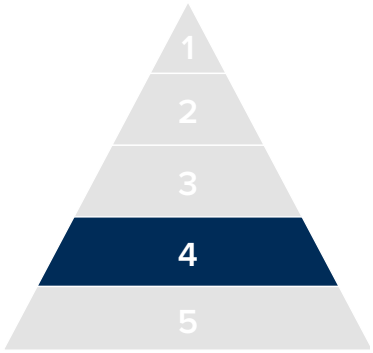
In spring 2007 computer systems and networks in Estonia were subjected to a massive distributed-denial-of-service (DDoS) attack which emanated from abroad. Government services such as the Ministry of Defense email network, as well as private services like bank websites and ATM networks, were disabled, rendering most public or private business effectively impossible during the roughly 48 hours of the attack. No physical damage occurred. Nevertheless, the attack intermittently paralysed financial and government activity in the country for a period of a few weeks. The episode illustrates the root dilemma of access: societies most adept at leveraging the internet for social and economic gain are those most exposed to cyber threats because their potential impact on society is so much higher. As the number of access points in a society increases, the vectors of attack for an opportunistic attacker to travel also rise. Access is both a vehicle for gain as well as a conduit for novel and unforeseen hazards.

Rather than recoiling from their deeply embedded internet use, the Estonian government and private sector used the incident to learn how to better protect their operations. With public-private cooperation, Estonia has fortified electronic signatures, electronic failsafes, firewalls and backup systems, and has become a champion of the cybersecurity agenda within European Union institutions and abroad. NATO's Cooperative Cyber Defence Center of Excellence sits in the Estonian capital, as does the EU's newly created IT Agency.

Estonia's digital ID cards are a core pillar of its cybersecurity strategy. President Ilves observed that when he first mentioned Estonia's ID card system to "Anglo-Saxon government officials, they opposed [it with] the classic Big Brother argument." And yet that system has proven -- so far -- remarkably resilient to exploitation; in fact, the effective use of public key cryptography has enhanced the security of authentication procedures. The digital ID system is the vital element with which Estonian citizens access over 300 essential services securely, remotely and instantaneously.

Resilience: Putting the User at Ease

Once users have access to the internet, the next need that they will seek to satisfy is resilience. This report defines resilience as consistent, dependable and reliable access to the internet or internet-based services with low risk of failure, even in the case of manmade or natural disasters. With resilience, the internet can expand beyond being useful for an individual to being vital for society as a whole. Only when the internet is resilient does it make sense for governments or businesses to rely upon it for critical infrastructure support or essential service delivery -- interrupted access is not good enough.



Resilience

In seeking to satisfy the need for resilience, we can consider both individual and systemic actions:

Individual resilience

At its most basic, resilience can come through enabling people to innovate and create their own solutions to business, technical or security problems that might otherwise interrupt access. It could also include the freedom to adopt heterogeneous third-party innovations and solutions as they require. Some user-level innovation and flexibility can create economic benefit and greater security across the internet with solutions developed for one sector applied in other industries or service provision.

Resilience at the user level comes through enabling people to innovate and create their own solutions, which can also result in economic benefit and greater security

One notable example of user-level resilience took place in the aftermath of Hurricane Sandy, which hit the US eastern seaboard in October 2012 with devastating effects. For instance, electricity and telecommunication services were heavily disrupted, forcing inhabitants of Red Hook, a coastal community in Brooklyn, to improvise. They responded by constructing an internet-linked 'mesh network' to communicate with the outside world while they waited for primary services to be restored. Mesh networks make the process of setting up spontaneous networks easier, which is particularly useful in a crisis. This is because mesh networks function differently than a hub-and-spoke network. If a hub fails, its spokes lose connection, but a mesh network is comprised entirely of spokes, so users can easily acquire an alternative route to the internet. This concept of avoiding a single point of failure from the design and concept stage is a recurring cybersecurity best practice at all levels of the hierarchy.

Resisting network or application designs with single points of failure and identifying appropriate and cost-effective ways to introduce redundancy (eg network connectivity, data replication, server failover) is a key part of responsible internet-based service and application design, especially for critical infrastructure systems.

Other solutions are being developed to deal with problems of unreliable internet infrastructure faced by many users around the globe. The Kenyan non-governmental organization (NGO) Ushahidi is developing the BRCK, a portable device that can switch between ethernet, wifi and mobile phone networks and supply a connection even when users experience loss of power or service.[14] These robust connection initiatives are often initiated by NGOs or the private sector and demonstrate leading-edge possibilities for user empowerment, resilience and security. For user-level resilience, the government's efforts may be best used to foster an enabling environment for user innovation.

System-level resilience

Where scale is a priority and regulatory or legislative constraints are more relevant, the government has a greater role. Ensuring resilience at the system level (either within or across critical infrastructure sectors) is of fundamental importance for tapping into the potential of the global internet.

System-level resilience can be understood better, and therefore improved, by asking where scarce resources should be deployed on the spectrum between recovering faster and never failing. This is particularly apt for critical infrastructure, and for making decisions regarding what is most critical. Faster recovery means using resources to bring 'mean time between recovery' closer to zero. The other end of the spectrum involves using resources to push 'mean time between failure' towards infinity. Both actions cannot be prioritized at the same time, but the position on the spectrum that is chosen will have a significant effect on the resilience and reliability of the internet or internet-dependent services. Similarly, what degree of interdependence on other critical infrastructure systems is acceptable and how is the risk of cascading failure mitigated or insured against? Are private or public organizations adequately incentivized to understand, disclose and mitigate risk, especially for regulated utilities?

Cybersecurity's role in bolstering resilience

As governments move more critical systems to the internet, their responsibility to protect them from attack -- and their accountability to citizens to enable resilience at user level -- will grow. At the resilience level of the hierarchy, the greatest cybersecurity need is to protect against coordinated attacks by malicious actors, possibly other states. Unlike conventional military hostilities, cyberattacks present new challenges for states in that it is difficult to quickly identify the aggressor, their location or their motivation. Furthermore, cyberattacks are often asymmetric, meaning that relatively low levels of resources are needed to inflict serious damage on a network relative to the costs of using traditional weapons. Non-state actors (for example, 'hacktivists') also add to the destabilizing nature of such threats.

Resilience is increasingly valued in such a complex environment, and high levels of interdependency between markets and organizations means that attacks and accidents alike are inevitable. This is even more pressing as thousands of public utilities, investor-owned utilities, service providers and customers increasingly interact in the digital space, drastically increasing threat vectors for critical infrastructure systems such as energy or water.

14 Forbes, "BRCK Keeps The Internet On When The Power Goes Off, Even In Africa", 5 May 2013

Financial markets -- critical to economic health -- are also under growing threat. The 2012 annual report of the US Financial Stability Oversight (FSOC) highlighted cyber risk as a priority issue and the Bank of England is working in cooperation with UK financial firms and government agencies to shore up their resilience against evolving cyber threats. US President Barack Obama included a warning about international hacking against the banking industry in his 2013 State of the Union address. In July 2013, Wall Street's biggest trading group, the Securities Industry and Financial Markets Association (SIFMA), organized a cyberattack drill called 'Quantum Dawn 2' that was designed to test the resilience of US banks. Participating members included JPMorgan Chase, Bank of America and Citigroup as well as government agencies like the US Treasury and the Department of Homeland Security.

The consequences of an effective, prolonged cyberattack which disrupts critical infrastructure and financial services will continue to rise, increasing the potential value to state or non-state actors seeking to disrupt industrialized countries and their economies. The challenge remains; to strengthen system-level resilience during the expansion of online services and transactions, while empowering users to make the most of the digital domain.

The challenge remains; to strengthen system-level resilience during the expansion of online services and transactions, while empowering users to make the most of the digital domain

The government's role at this level involves establishing capabilities and processes for responding to cybersecurity incidents in key internet dependent sectors of the economy. This includes the establishment of national authorities for coordinating cybersecurity incident response and testing the readiness of their capabilities to ensure resiliency. Resiliency also requires readiness: response organizations and processes should be tested regularly, as with the Quantum Dawn 2 drill, to ensure that they are ready to respond to a variety of incidents that could negatively impact resiliency.

International standards and best practices can also improve resilience. Government policymakers should look at the best way to leverage international risk management standards and best practices to improve resilience in government and critical infrastructure operations. Recent efforts by the National Institute of Standards and Technology (NIST) to collaborate with the private sector to build a coherent cybersecurity framework, based on international standards that can be adapted to meet the unique risk profiles of enterprises, is a seminal undertaking. Recent European Union efforts to identify standards and best practices could also benefit broader international efforts. Greater adoption and use of international standards and best practices also helps create more harmonized approaches to cybersecurity and more opportunities for collaboration on resiliency at the international level.

The case study that follows explores the experience of online critical infrastructure systems, both in terms of potential gains and possible risks. At the resilience level of the hierarchy, the cybersecurity needs move from the individual to the systemic, and the government takes on a more comprehensive role in ensuring its service provision is resilient against cyber threats.

CASE STUDY: CRITICAL INFRASTRUCTURE SYSTEMS

Internet networks must be considered resilient before they can support critical infrastructure. The safe handling of energy systems, nuclear stations and water delivery is of utmost importance to the citizens and enterprises that any state is accountable for. And yet the presence of critical infrastructure systems online opens a range of cyber exposures. Sophisticated attacks on critical infrastructure are a particular risk given extensive current system vulnerabilities, potential for disproportionate impacts, and common connections between control and data-sensitive networks. Developed countries, which currently use the most connected infrastructure, are the leading targets for such attacks, with the energy sector as a particular focal point.

Security is critical

There are a range of critical infrastructure systems that are both vital to socio-economic functions in modern society and highly susceptible to cyberattack. Critical infrastructures are defined differently by every country, but generally include:

- energy;
- banking;
- telecommunication;
- transportation (air, rail, shipping and other civilian transport networks); and
- other essential service provision systems like water, healthcare, chemicals and public safety.

In terms of realizing the potential of the internet, critical infrastructure systems stand to gain massive system-level operational efficiencies and improve reliability as information networks are more closely coupled with the underlying physical delivery networks in operation. For the electric power system, which must solve large physical “powerflow” models of the physical system to adjust pricing and dispatch generators on the network in short increments, huge amounts of computing power can enable better wide area management, planned maintenance, outage response and service restoration. In turn, this can provide better power quality and lower actual costs to end-users. Large-scale power outages such as the historic Indian power outage of July 2012, which affected half of India’s population, have helped to further increase utility industry interest and awareness of infrastructure system monitoring for wide area network management in developed and developing countries alike.

Rich targets

The electric power industry is a useful lens through which to evaluate critical infrastructure cyber risks, especially given the drive for a digital transformation to a 'smart grid'. Due to the high capital cost of energy industry infrastructure, limited software/firmware updates and the lengthy design service life of many components, current critical infrastructure systems are likely to be more susceptible to the full spectrum of potential cyber threats. Moreover, these systems tend to remain vulnerable for longer time periods following publication or release of exploits to such vulnerabilities as a result of limited automated capabilities and patch management difficulties.

Energy focused organizations have historically been rich targets for exploitation because of the multiple data types utilized to provide services, the visible political and social impact of successful compromises, and a legacy of difficulty in properly defending against attacks. In the first half of 2013, the US Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team responded to over 200 incidents across all critical infrastructure sectors with five on site deployments that involved attacks from sophisticated threat actors.[15] The majority of the incidents (53%) were in the energy sector. This is in line with 2012 trends, which exposed several vulnerabilities in the energy sector, including:

- the use of publicly available search tools like Shodan[16] to tap into internet-accessible industrial controls and networking equipment, including systems that automate power grids;
- the widely publicized Stuxnet and Flame[17] cyber espionage efforts in Middle Eastern countries; and
- the Shamoon virus. Though not as well publicized as Stuxnet or Flame, Shamoon wiped out hard drives, sent compromised information to the attacker and prompted Saudi Arabia's national oil company, Saudi Aramco, to shut down its operations for a week in August 2012.[18]

These are all illustrations of recent network exploitations or exploitation tools that make use of energy and other critical infrastructure system vulnerabilities.[19]

Electric utilities and oil companies will remain prime targets, especially as these industries move towards smart metering. New approaches are required to manage operations, secure the network and identify intrusions that happen as soon as possible. Such approaches will be necessary to protect valuable intellectual property and sensitive information like that targeted in the Night Dragon attacks[20] on petrochemical, energy and global oil companies as well as actual operational control systems.

15 Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team ICS-CERT Monitor, April/May/June 2013
16 Shodan is a search engine that lets users scan about 500 million connected devices and services like servers, webcams, routers and other internet-connected systems.
17 While Flame was primarily an information gathering tool, its capabilities provide sophisticated means of gaining access credentials, information, network topology and so forth relevant to critical infrastructure systems including energy, water and finance that are of interest to the originating party.
18 Shamoon damaged approximately 30,000 machines.
19 Symantec, 'Symantec Internet Security Threat Report', 2013, vol. 18, p 5
20 In the Night Dragon attacks, hackers stole sensitive intellectual property from energy companies using relatively unsophisticated methods. McAfee, 'Global Energy Cyberattacks: Night Dragon', 2011

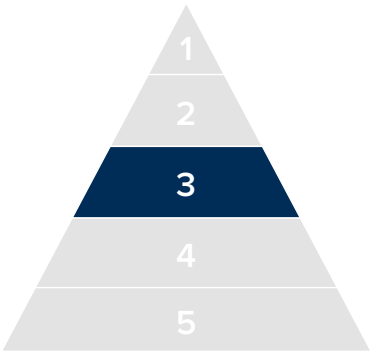
Modernizing critical infrastructure IT systems by leveraging the cloud

While cloud computing remains a relatively new technology for most critical infrastructure enterprises, the growing knowledge base and technological capabilities to responsibly manage failover and provide adequate redundancy are key components of using the cloud to improve infrastructure operations. In many cases, cloud-based deployments can reduce IT costs and may reduce overall risk of system failure or long-term outages. In addition to reducing risk, cloud services can help realize a greater portion of the internet's potential to support critical infrastructure. Through improved modeling, automated metering and enhanced control systems -- many of which are enabled by cloud computing -- the US economy stands to gain 130 billion dollars in additional value annually by 2020.[21] These benefits are only possible when the network is resilient.

21 Benefits are categorized into customer applications, advanced metering infrastructure and grid applications. McKinsey & Company, 'US Smart Grid Value at Stake', 2010

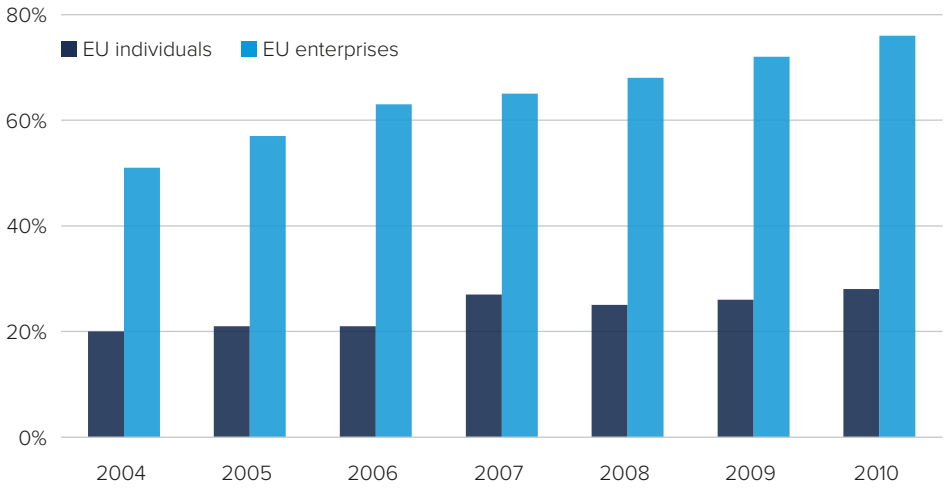
Connectivity: Making Links

Our notion of the need for "connectivity" goes beyond just the user's opportunity to access the internet as described in the first level of the cybersecurity hierarchy: it encompasses the need for users to connect with relevant and important social and economic services (for instance healthcare, education, voting, tax collection and so forth). At this stage in the hierarchy the end-user takes for granted that they will have access to the internet and that it will be reliable. In other words, connectivity represents an expansion of the notion of access delineated above: not just access to the internet, but rather a connection to critical functions *through* the internet. This maps loosely to Maslow's need for a sense of belonging to a group.



This is an issue of growing importance for governments as channels of communication with public authorities increasingly revolve around the internet for both individuals and enterprises (see Figure 5). This holds true of almost every area of public life, from tax filing and business registration to receipt of social welfare benefits and political lobbying.

Figure 5: Use of the internet for interaction with public authorities (% of total)



Source data from Eurostat, 2013

We can think of connectivity in terms of both:

- **The internet of people.** In the next 20 years, the internet will expand far beyond its current 2.3 billion users, and the majority of humankind will be connected in some way via the internet.

- **The internet of things.** Rapid proliferation of internet-protocol enabled devices is changing business processes and lifestyles alike. By 2015, the number of internet-connected devices is predicted to be more than twice the world's population.[22]

Interpersonal networks via the internet enhance users' ability to gain personal value from their connections. Disparate individuals can link up to form more powerful interest groups. People in remote areas can have a voice in city centers. Banks can tap into large groups of customers with low banking thresholds, creating a valuable market where before there was none (as well as creating an opportunity for unbanked customers). Patients can connect with care providers without having to step inside a hospital. Governments can disburse benefits directly to individuals with fewer intermediaries and transaction costs. The potential for the state, enterprises and individuals to reap value from connections made on the internet is enormous.

When conceiving of connectivity in a global context, the availability of local language content and the ability to communicate to local language groups and people are also important. In other words, once we get to the connectivity level, we start to see regional divergence and local context becoming more significant -- compare, for example, the connectivity potential for an English or Chinese speaker versus a Mongolian or Swahili speaker.

Cybersecurity and connectivity

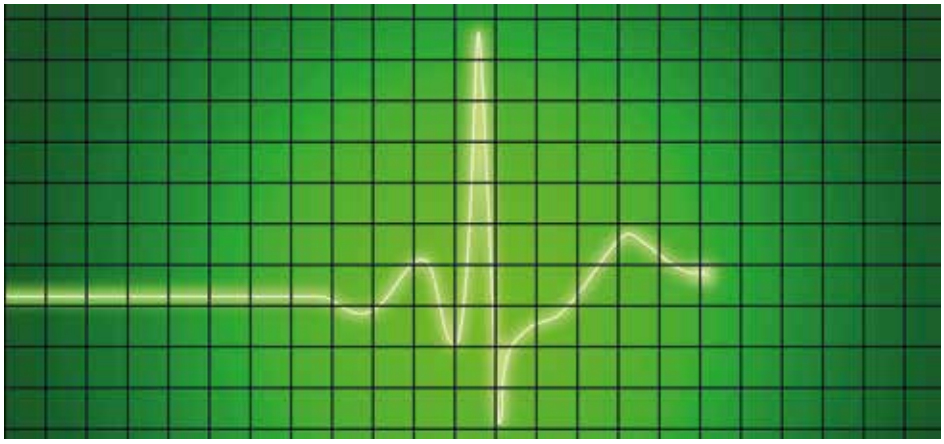
As the level and sophistication of connections increase, so too does the need for security around those connections. When users begin to transmit financial data, health information or sensitive commercial information, the priority of cybersecurity drastically rises. Connectivity between users, machines, applications and data means that threats are no longer linear, but reflect a mesh of interconnectedness.[23]

Internet transactions and interactions can thrive when they are secured. Government policymakers are increasingly appreciating that the internet is more than a mechanism for e-commerce and social media, but that high value transactions rely on the health of the internet. Telemedicine, e-banking, e-government and more can only flourish when the cybersecurity of these connected transactions can be assured to an acceptable level. To do this, governments need to work closely with the private sector to address fundamental challenges that enable the security of such transactions, including trusted identities, data, applications and devices.

Beyond policy action, technical measures should also support safe end-user access. Going back to the earlier case of Estonia (see Part I), the country's national ID-card system demonstrates that technical remedies can be employed to promote and support end-user security. It has provided a robust layer of protection for access to financial and government services, ranging from to tax filing to voting to the use of health services. The system applies simple but resilient principles of public key cryptography. Moreover -- and remarkably, in comparison to similar national ID-card schemes -- the Estonian system records all requests for user data, which facilitates the detection and forensic investigation of unauthorized or inappropriate access.

22 Boston Consulting Group
23 Charney, S., Microsoft, 'Trustworthy Computing Next', 2012

The case study that follows highlights mobile health -- an example of creating value through the internet by connecting users to critical services and an illustration of the role that cybersecurity plays in boosting that value. Governments, traditionally accountable for enabling the delivery of critical health services, can support innovative technological solutions by securing the cybersecurity structure around them.



CASE STUDY: M-HEALTH

The widespread adoption of mobile technologies offers low-cost and innovative solutions to global health challenges. The use of mobile technology in disease prevention, diagnosis and monitoring will be increasingly relevant as the global disease burden shifts to long-term chronic diseases while governments worldwide try to curb healthcare expenditure. The value of m-health lies in the connection between patient and provider, which in turn rests on the security of the network to transmit and store our most personal dataset -- our health information. Governments can benefit from creating a secure environment in which mobile health (m-health) can thrive, making healthcare delivery more efficient and more accessible for citizens and enterprises.

Three trends combine to bolster m-health

There are three concurrent trends driving the use of mobile health (m-health), defined by its use of wireless communication devices to support public health and clinical practice:

- The pervasive and growing use of mobile telephones and devices;
- The increase of chronic diseases that require ongoing and frequent care delivery or monitoring in both the developed and developing world; and
- The need for relatively low-cost solutions amid tight fiscal budgets.

This is especially true where countries have seen their health expenditures escalate amidst economic stagnation; in the OECD as a whole, health costs have been rising faster than economic growth. To offset this, public health organizations are promoting low-cost technologies, in particular e-health -- defined by the World Health Organization (WHO) as “the cost-effective and secure use of information and communications technologies in support of health and health-related fields.”

M-health can be seen as a subset of e-health, in that the digitization and ICT necessary to enable mobile monitoring and reporting are related to those in e-health, such as electronic patient records and health information exchanges. M-health includes the use of mobile phones, wireless communications with large medical devices, remote sensors worn by patients and passive data collection. For example, India’s effort to assign twelve-digit electronic identification numbers to 1.2 billion people aims to provide access to basic health and welfare services through online and mobile platforms.

The value is in the connection

The development of m-health illustrates the need for internet connectivity because the value-added is in the health services users are able to access from organizations via the internet. The importance is the connection and interaction between the patient and their network of health providers, insurance companies and government services. Mobile internet makes this possible in a way that was hard to imagine before the spread of smartphones and broadband. All segments of the population can benefit from the connectivity provided by m-health, though it will be those who are the least connected to health services in the analog world that will see the most marginal benefit.

Higher-tech solutions, like applications (apps) designed for smartphones, will naturally have better traction in more developed countries. However, lower-tech apps that rely more on SMS communication can have a significant marginal impact in a developing country. Take the example of a diabetes program that can text reminders to a patient about taking blood tests, and then collect the results via text for monitoring. Such programs are already proliferating. There are an estimated total of 40,000 health-related apps, and they are increasing. The WHO and the ITU launched an m-health joint initiative in 2012 to promote the use of mobile technology -- chiefly text messages and apps -- to combat chronic diseases. Aetna, a leading US insurer, has launched a healthcare app store for mobile phones. The Gates Foundation works closely with program partners to align ICT platforms wherever possible, while Voxiva, a privately held interactive m-health company founded in 2001, acts in markets from Peru to Rwanda, Mexico and the United States.

SMS intervention is also advancing maternal health and taking advantage of synergies with m-banking. Mamakimba is an early-stage program that works in Kenya to inform and encourage expectant mothers to save for pre- and ante-natal care. Women can use their M-Pesa accounts to open a savings account, be informed about the costs of a next visit and have the fee deducted from the account upon completing the visit. Women also receive advice on maternal health through SMS.

Securing our most personal dataset

The rise of m-health means that increasingly large amounts of private health data will be travelling between mobile devices and servers, through the cloud and into a range of disparate medical ICT systems worldwide. Along with financial data, health data can be considered as one of the most private datasets a person has -- a breach of privacy would seriously undermine the confidence in mobile systems, thereby limiting their utility. But along any individual's care pathway, there may be dozens of physicians, clinics, hospitals, diagnostic centers and laboratories that will need to access sensitive data. Data may be collected and communicated starting from devices in an emergency vehicle, to diagnosis in the hospital, to follow-up treatment in the home. Each point represents a valuable data collection opportunity, but also a potential vulnerability if communications are not secure. The current situation is exacerbated by proprietary solutions and outdated approaches, leaving security management weaker than it should be.[24]

Privacy based on privilege management, authorization, anonymization as well as accuracy, accountability and auditability is crucial for the functioning of m-health.[25] It is also important to consider m-health cybersecurity from a regulatory perspective. Though there are rigid legislative mandates around health data in some countries, others may not have a robust protective framework -- and all countries lag in their current regulation of mobile health.

24 Pharow, P., Blobel, B. 'Mobile Health Requires Mobile Security: Challenges, Solutions, and Standardization.' eHealth Beyond the Horizon; Get IT There - Proceedings of MIE2008; The XXIst International Congress of the European Federation for Medical Informatics, IOS Press, pp 697-702

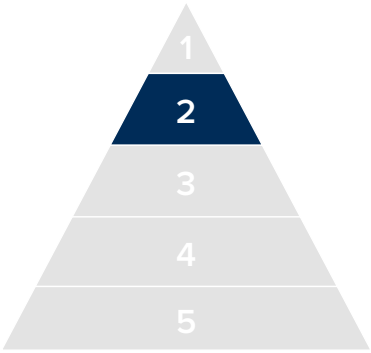
25 Ibid.

The US Food and Drug Administration is currently working on final regulatory guidelines for mobile health applications, which means that the area will come under increasing federal oversight in the US and potentially elsewhere once the precedent has been set.

Although other significant obstacles remain -- hardware customization, interoperability and financing among them -- governments will continue to seek to increase the flow of ICT investment into the health sector through legislation and program funding. Therefore, the need to ensure the security of health information will grow in tandem.

Trust: Sharing Private Data

At this level, access to the internet is robust and widespread, the networks being utilized are resilient, and users are engaging with significant counterparties over the system. In other words, the internet is considered reliable, relevant and transactional. The predominant need for users at this level, then, is to trust the internet. This is the level where many developed countries find themselves today, hence the robust and ongoing debate about the government's role in securing or undermining that need for trust.



At this stage, users go beyond the case-by-case decisions about trusting individual connections towards creating a trusted ecosystem.

The trusted ecosystem

There are many dimensions to creating trust. For example, trust is about the relationship among individuals; between consumers and service providers; among service providers; between governments and private actors; and among governments. Each of these dimensions make up the trusted ecosystem, and the government can have a role in fostering trust throughout.

Individuals

At the individual level, the need for trust has been heightened by the rise in people channeling different aspects of their lives -- work, home, financial, social -- through the same device, whether a smartphone, computer or tablet, while demanding a balanced mix of integrity and access, privacy and reliability for each aspect. In the most basic terms, users will seek reassurance that a given site is secure and not going to harm them and that the data they send will not be changed, deleted, falsified or used in a way that is against their intended purpose. This means the user is confident about their ability to secure themselves and understand their own security. A key aspect of this is making users aware of and able to recognize social engineering, as noted in the basic level of access, which remains an important part of knowing when and where to trust online connections.

Today, many trust decisions have technology-based solutions. As networks have developed, most of the verification needed to allow new entities to join is done instantaneously through software, so that much of the concern about the integrity of the system is lifted from the user. The invisibility of the processes of a 'trusted provider' makes risks still harder to assess; risk managers therefore place considerable emphasis on externally assessed

process certifications such as ISO. In many cases, programmers have embedded their own definitions of 'trust' into their software (done primarily through the use of digital certificates) and remove human decision-making from the situation, for better or for worse.

Consumers and service providers

Government has a role in creating safety nets that encourage trust online. Once these safety nets are in place, users feel secure in sharing their data and taking advantage of internet channels for personal, professional and commercial purposes. The case study in this section explores the explosion in e-commerce. A key driver of this industry (and an indicator of the importance of trusted safety nets) was an act by the US Congress to limit consumer liability for online credit card transactions to 50 US dollars. Assured that they could trust this policy to protect them online, consumers could make more use of the internet's potential to revolutionize commerce.

Governments and their citizens

Agreement on transparent standards of appropriate state behavior online -- particularly with respect to the appropriate balance between national security and user privacy -- is important

In the end, online trust is about more than user-verification and consumer protection policy. The trust dimension between governments and their citizens is also of utmost importance in creating a trusted ecosystem. Agreement on transparent standards of appropriate state behavior online -- particularly with respect to the appropriate balance between national security and user privacy -- is an important area of consideration and action for governments. Relatedly, businesses are a third pillar of the relationship between citizens and the public sector through the provision of online services. The boundaries and terms of these interlinked relationships must be transparent to all parties involved to establish and maintain trust. However, this trust-building cannot come just from the governments themselves: given the role of the private sector in developing, refining and operationalizing existing confidence-building measures (eg vulnerability disclosure management, secure development of code and adequate reporting of government requests for user data), it is only reasonable that industry representatives and citizen representatives be included in the effort.

Government to government

Trust-building between governments is also a growing need. Cybersecurity has emerged as a serious international diplomatic issue as political leaders grapple with how to establish norms or delineate the accountability of national governments for cyberattacks across borders. These issues will only gain in prominence in bilateral and multilateral relationships. For example, the biannual US-China Strategic and Economic Dialogue, held in July 2013, featured the first Cybersecurity Working Group. Washington and Beijing pledged to enact "practical measures" to enhance dialogue on international cyber rules and norms, and indicated their desire to enhance coordination and cooperation between their respective Computer Emergency Response Teams. Internationally, it is likely that progress on these issues will be incremental with regular flare-ups as new hacking attempts occur -- however, increased dialogue can help build trust between nations and avoid dangerous miscalculations or misjudgements that lead to conflict.

The case study that follows highlights two industries that have shifted almost entirely from an analog to digital domain -- commerce and telecommunications. These transformations are only possible when the actors involved had a high level of trust in the internet services that underpinned the new infrastructure of their businesses. In the same way that service providers must trust that the internet can support their business, the end-users must trust that their transactions will be secure or there would be no market to serve. For the government, the imperative to create a secure operating environment is fundamental to foster this trust and allow for the ongoing move of new industries to the digital world, where they can fully exploit the potential of the internet.

CASE STUDY: DIGITAL TRANSFORMATIONS

While many industries have made the move from the analog to digital environment, some of the most remarkable transformations have been in commerce and telecommunications. The sheer volume of growth in these industries demonstrates a high level of trust in the internet to securely deliver goods and services. That degree of trust would not be possible without the cumulative satisfaction of the other levels of the hierarchy: access, resilience, connectivity. For these two industries, as access, resilience, connectivity and trust increased, interactions that were previously economically or technologically impractical became feasible as speeds rose and costs fell. The analog to digital transformation has not just aided in increasing profitability or end-user value, but it has actually helped grow the pie by providing efficiencies to multiple actors, including the state. Thus, the state has an interest and an imperative to ensure the security of the digital domain to foster and promote the ongoing growth of its digital economies.

Digital sales of physical goods

The massive growth in e-commerce remains one of the most visible illustrations of this broader digital transformation. The size and scope of the e-commerce revolution is particularly remarkable considering that the internet was opened to commercial activity in the United States only in 1991 and that even hyper-text transfer protocol was only standardized as HTTP v1.0 in major internet browsers in 1996.

In this context, consider that first quarter sales in 2013 for Amazon reached 16 billion dollars, marking a 22% year-on-year growth, while that of fellow e-commerce heavyweight eBay reached 3.75 billion dollars. The growth in online sales of physical goods by companies such as Amazon and eBay are the result of the efficiencies made possible by IT breakthroughs enabling secure business-to-consumer and business-to-business transactions at extremely low margins and underpinned by on-demand logistical services delivered at a scale and cost unimaginable 20 years ago. The end-user's trust in the system is both critical to and a result of the high-functioning of the system. A notable example of transaction-enabling technology is Amazon's '1-click' service where a buyer's prior submission of payment and shipping information allows the purchase of a product in one step.

While US-based companies have been the pioneers of e-commerce, growth among e-retailers in other parts of the world is quickly gaining traction, due both to technological advancements and rising incomes. Since 2003 e-commerce in China has grown at a compound annual growth rate (CAGR) of 120%, and in 2012 the market brought in an estimated 210 billion dollars in revenue.[26] Alibaba, China's e-commerce giant, hosts business-to-business, business-to-consumer and consumer-to-consumer sales, and revenues in the first nine months of 2012 reached 4.1 billion dollars.

First quarter 2013 retail e-commerce sales topped 50 billion dollars for the second time on record

The global spread in the popularity of and trust in e-commerce is set to continue. First quarter 2013 retail e-commerce sales globally topped 50 billion dollars for the second time on record, raising hopes that total sales for 2013 will exceed 200 billion dollars and extend an extraordinary period of growth that has remained above 9% year-on-year since Q1 2010.

E-commerce will become increasingly commonplace as companies release new enabling technologies to attract a growing consumer base and engender greater trust. For instance, Square's reader permits credit cards to be swiped using a mobile app; it also offers the 'Wallet', which allows users to store payment information in their phones, pay with a mobile app and store receipts. Intuit's GoPayment provides the same service, and eBay's PayPal is also vying to enter this mobile-enabled virtual commerce space. New technologies as such continue to push the boundaries of e-commerce, increasingly facilitating the digital sales of physical goods.

Telecommunications go digital

The telecommunications industry is another good illustration of what happens when a sector moves from analog to digital systems by applying information technology to physical industries. Telecoms has evolved from manually intensive exchange switchboards in the early twentieth century to the large spaces originally required for exchanges, to automated switching and networking. This networking now supports interoperability for multiple generations and technology platforms across numerous global providers via increasingly standard protocols.

To take just one example, the development of the automated switching technology used for connecting international long-distance voice and fax calls comprised roughly 69 billion dollars of the 850 billion dollar global telecommunications industry in 1999. With massive investments in capital infrastructure (eg transoceanic fiber) operating below capacity, carriers negotiated directly with each other to trade minutes, rents, maintenance fees and service fees at hubs. A large opportunity emerged to provide less costly routing services for telecommunications networks by connecting buyers and sellers to an anonymous exchange to protect confidential capacity information while injecting much needed liquidity to the market. Arbinet, an international voice and IP service provider, set up an international spot market and exchange for wholesale voice minutes.

26 Chang, E., Chen, Y., Dobbs, R., 'China's e-tail revolution', McKinsey Global Insight Report, March 2012

By reducing the transaction costs for carriers and resellers, providing quality assurance monitoring for buyers and sellers, and anonymizing the process, Arbinet and its competitors completed the transition from a manual switch to a fully automated international market; the transition enabled daily, hourly, 15-minute and eventually real-time trading of excess voice capacity. Costs for long-distance and international calls fell dramatically as increased liquidity enhanced competition and services into the early 2000s.

Skype and other internet-protocol based voice, chat and video services are a more recent evolution that further disrupted traditional service providers. Unencumbered by existing infrastructure and able to leverage network access and resilience which had reached sufficient density, Skype's ability to piggyback on the internet -- the architecture is a hybrid peer-to-peer and cloud model, as Skype's supernodes moved into Microsoft's global data center -- to enhance human connectivity without utilizing traditional voice infrastructure drove additional change and telecom business model innovation.

Skype's new service delivery model was impossible with dial-up internet services

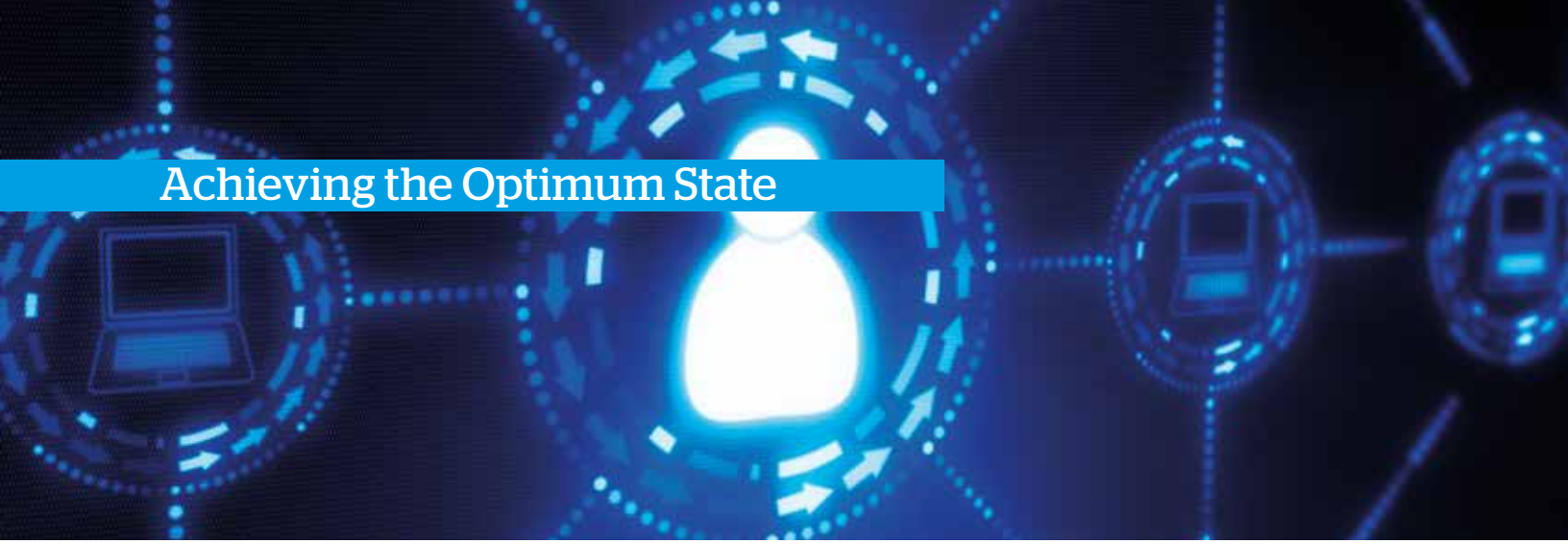
This new service delivery model was impossible with dial-up internet services. Its introduction was enabled by "always on" broadband internet access and soon grew to disrupt existing video teleconference and file transfer business models when the incorporation of web cameras connected individuals at long distances like never before. The low-cost delivery method for Skype-to-Skype calls, connections to traditional landlines, multiple permanent international phone numbers, and additional organizational features helped the service grow to capture more than 30% of the international call market share in 2012.

A cumulative process

The transformation of analog systems and industries to those enabled and enhanced by information technology systems is an additive process, and one that is made possible by the security conditions it develops in. The cumulative gains enabled by growing digital infrastructure and captured data allow for previously unattainable or undiscovered efficiencies in numerous existing business areas and occasionally provides the basis for the creation of entirely new services and products. Additional analog to digital transformations will continue to proliferate as people increasingly trust the internet and as business models increasingly target specific subsets of the market with specialized services and products. Businesses will be able to do this thanks to available tools such as social networking that can reduce customer acquisition costs and enhance end-users' ability to find relevant services and products.

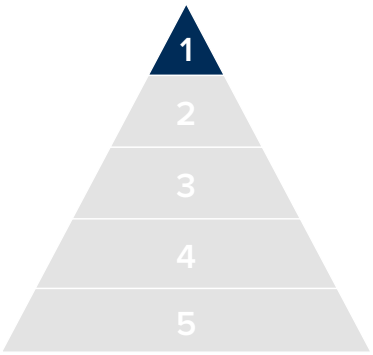
The cumulative gains enabled by growing digital infrastructure and captured data allow for previously unattainable or undiscovered efficiencies as well as the creation of entirely new services and products

Furthermore, as additional industries capture data about processes, customers and operations, data-mining and analysis is consistently aiding industry experts in optimization and focused research and development into new technologies and services reducing or eliminating friction points. Improvements in network and data security are increasingly necessary to keep pace with these advancing commercial opportunities, in particular as they expand into emerging markets with different (and often less robust) legislative, regulatory and judicial environments. At the same time, this raises serious questions about user privacy that return us to the basic question of trust.



Achieving the Optimum State

At the top of Maslow's hierarchy of needs is "self-actualization". Maslow describes this level as the desire to accomplish everything that one can, to become the most that one can be.[27] Individuals may perceive or focus on this need very specifically. For example, one individual may have the strong desire to become an ideal parent. In another, the desire may be expressed athletically. For others, it may be expressed in paintings, pictures or inventions.[28] In the cybersecurity hierarchy of needs, we think of this as the "optimum state".



This state is where the hierarchy of cybersecurity needs related to access, connectivity, resilience and trust all culminate in security to enable creativity, innovation and opportunity.

The optimum state

In the same way that Maslow did not envision that most people would reach the top of his pyramid, neither do we postulate that perfect security has to be achieved in order for individuals and businesses to gain significant amounts of value from the internet. Nor do we assume that once the optimum state has been achieved that it is automatically sustained. It is a flexible and ongoing state of flux that reflects the evolving environment and the actors within it. However, it is in the aspirational pursuit of this goal that we can prioritize, focus and push the frontiers of what we are capable of achieving in the digital world.

What might be possible if all the needs in the pyramid are met? Below are just a few examples of how the internet's potential can be more fully realized to improve the day-to-day welfare of individuals, organizations and governments:

- Cloud computing, elastic infrastructure and the internet of things will continue to encourage experimentation with new technologies, service offerings, business models and will allow unprecedented introduction of new businesses at remarkable scale with limited capital investment.

- The automated home, already a reality, could be more widespread with huge energy savings, cost implications and home security benefits. Urbanization and the rise of a new global middle class will continue to boost energy consumption per capita, and smart metering and other home automations could be essential in coping with this rise in demand.

27 Maslow, A. (1954). Motivation and Personality. New York, NY: Harper. pp 92
28 Ibid. pp 93

- Predictive maintenance has already saved some companies hundreds of millions of dollars -- in the case of logistics companies by implanting sensors in their fleet of delivery vehicles which send alerts when a part will break before it actually breaks. These gains could be realized across a range of sectors including automotive, manufacturing, utilities, transportation, aircraft and more.

- Data-driven personal health and fitness could lengthen lifespans, prevent or contain disease and personalize care in a way that we are only beginning to understand. When national (or even international) health databases can be safely combined, anonymized and analyzed, we can reveal population-level medical insights based on enormous datasets that reveal what clinical trials may not.

- From a public safety perspective, road safety is an interesting example. Temperature sensors on every street lamp could provide data on road conditions, warn about ice and allocate snowplow routes to prevent fatal accidents. Legislation is already emerging in the European Union that will require all cars to be equipped with a cellular data network so that emergency services can be alerted automatically in event of an accident. Self-driven cars, completely reliant on data systems, are also on the horizon.

These innovative uses of data will thrive in the internet's optimum state, but would be critically undermined -- and even destructive -- if the cybersecurity of the collection, transmission and processing of this data is compromised

All of these innovative uses of data will thrive in the internet's optimum state, but would be critically undermined -- and could even become destructive -- if the cybersecurity of the collection, transmission and processing of this data is compromised. This list of day-to-day applications can even be expanded to include the international level disasters that could be avoided by establishing clearer cybersecurity standards and norms, avoiding miscalculations or misjudgements that lead to open hostility.

A more secure future requires a balanced approach

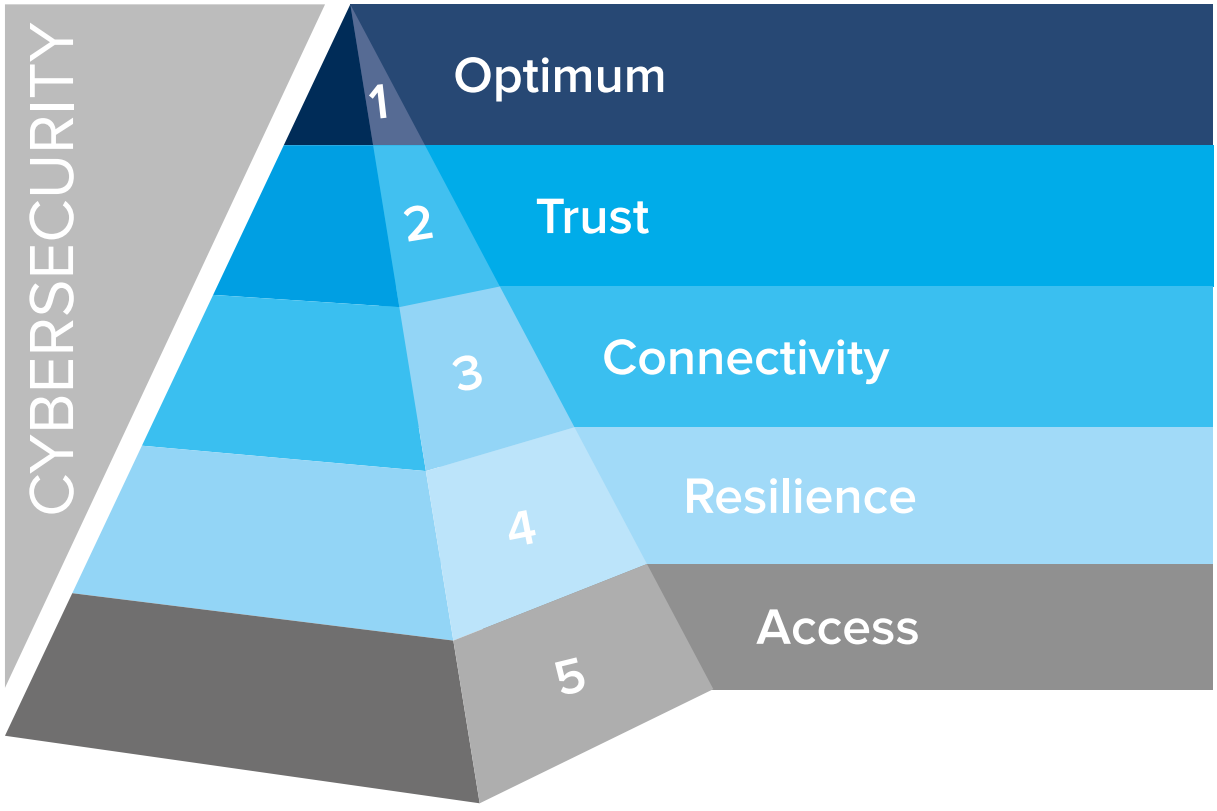
Achieving this optimum requires balanced tradeoffs between competing priorities with careful stakeholder involvement. The enduring challenge for governments is to develop a cybersecurity paradigm where the goal is to prevent malicious activity while maintaining an appropriate and responsive balance between usability, cost and exposure. Core to any effective cybersecurity risk management practice is a keen awareness that adaptability is the cornerstone of preparedness. The internet threat landscape is constantly changing. For this reason, the essential precondition of effective cyber risk management for the preservation of the optimum state of security -- once it is achieved -- is the ability to adapt to novel and unexpected security challenges.

Governments seeking to protect themselves, along with the welfare of individuals and organizations in their country, can best accomplish this by meeting the needs at each respective level of the cybersecurity hierarchy while focusing investment in an ascending order. Combined with focused direct investment and private partnerships to develop access, improve resilience, build connectivity, strengthen user trust and work towards a harmonized, transactive network, nation states can improve prospects for growth, governance and quality of life.

Thus, taking advantage of the potential benefit from the internet requires a balanced approach that maximizes the increase in each of the levels of the hierarchy and requires reasonable trade-offs between the needs of governments, individuals and organizations/enterprises -- in so doing, we reach the optimum state.

Recommendations

These recommendations are designed to assist governments in the provision of greater cybersecurity for their citizens, for organizations operating within their borders and ultimately for themselves. Naturally, nations will have to choose their own paths based on their individual context and goals, but the recommendations in this section should have a general usefulness in framing and prioritizing action across the hierarchy of cybersecurity needs.



5

ACCESS

Creating a legislative framework sets the scene for a secure internet environment.

It is often the case that technology advances more quickly than governments can create legislation and regulation to account for it. For countries that are undergoing a rapid expansion in internet access -- due to the removal of structural limitations or a concerted effort to build a development strategy around ICT -- the communications policy framework will be crucial in shaping the security environment. Cybersecurity policy can address laws, norms and values around cybersecurity, as well as foster capacity-building, rights of access for citizens and foreign cybersecurity policy for external threats. Fortunately, with a range of existing national ICT policy frameworks, governments can work with peers or advisors to implement known best practices or establish tailor-made policy for their national context. At the same time, the current international cybersecurity policy framework is fragmented and more competitive than cooperative. Therefore, governments at the 'access' level of the hierarchy will have to carefully consider their own security policies and where they fit into the international policy spectrum.

Improving end-user awareness of cyber threats is an essential investment for countries that are rapidly expanding internet access to citizens that previously had limited or no access.

Education and awareness campaigns may be just as effective as technical security responses in addressing basic access level risks. The expansion of internet access, the rise in the number of users and the growth in the number of connected devices, increases the potential targets for an opportunistic attacker to reach. In principle all new users (and the internet-related functions they perform) become, by virtue of access, viable targets for cyberattack or compromise. Communities that have only recently gained access to the internet may also be more susceptible to social engineering attacks, whereby seemingly legitimate emails deliver malicious code or convince recipients to give up information or to click on a malicious link. Government policymakers should work with the private sector to promote user awareness; and provide risk management guidance to individual users and small and medium sized enterprises. Campaigns such the US "Stop. Think. Connect." and the UK's newly announced 4 million pound cybersecurity awareness campaign can help inform users to manage the risks of internet access. Educational campaigns may be just as effective as technical security responses in addressing basic access-level risks.

Awareness promotion is a joint responsibility of users, computer manufacturers, software designers, service providers, company employers and governments -- and therefore requires a joint effort by all these players.

RESILIENCE

Improving threat response mechanisms is central to resilience.

4

Effectively addressing the hierarchy of cybersecurity needs with respect to resilience requires the establishment of capabilities and processes for responding to cybersecurity incidents in key internet dependent sectors of the economy. Government policymakers should ensure that they have established national competent authorities for coordinating cybersecurity incident response, adopted incident classification and tested the readiness of their capabilities to ensure resiliency. The role of the national competent authority is often fulfilled by the creation of a national computer emergency response team or "CERT" that can coordinate among government agencies and work with the private sector to address issues that might impact the reliability or availability of internet infrastructure within the country. Additionally, developing clear and consistent incident classification can help the CERT and its non-government partners better understand, analyse and respond to cybersecurity incidents. Finally, resiliency is closely related to readiness. Response organizations and

process should be tested regularly to ensure that they are ready to respond to a variety of incidents that could negatively impact resiliency.

International standards and best practices can improve resiliency.

International standards for risk management and best practices can assist public and private organizations in increasing resilience against disruptive or destructive cyberattack. Government policymakers should look at the best way to leverage international risk management standards and best practices to improve resilience in government and critical infrastructure operations. Recent efforts by the National Institute of Standards and Technology (NIST) to collaborate with the private sector to build coherent cybersecurity frameworks, based on international standards that can be adapted to meet the unique risk profiles enterprises, is an important undertaking. EU efforts to identify standards and best practices could also benefit broader international efforts. Greater adoption and use of international standards and best practices helps create more harmonized approaches to cybersecurity and more opportunities for collaboration on resiliency at the international level.

CONNECTIVITY

Internet transactions and interactions can thrive when they are secured.

3

Connectivity is where internet dependence is solidified. Government policymakers should recognize that internet is not just a mechanism for e-commerce and social media and create a policy environment that incentivizes more secure connectivity. High value transactions that rely on the internet -- telemedicine, e-banking, e-government and more -- can only thrive when the cybersecurity of these connected transactions can be assured. Governments need to work closely with the private sector to address fundamental challenges that enable the security of such transactions, including trusted identities, data, applications and devices. Addressing the hierarchical connectivity need requires both policy and technology frameworks. For example, the US National eHealth Collaborative (NeHC)[29] is a public-private partnership that enables secure and interoperable nationwide health information exchange to advance health and improve healthcare. NeHC's stakeholders include government agencies, health systems, health professionals, academic medicine, patient and consumer advocates, major payers and employers, non-profits, technology providers and others. A strong commitment to neutrality and multi-stakeholder engagement allows NeHC to offer a uniquely balanced perspective and platform for collaboration to accelerate progress toward the widespread and efficient use of health information technology and health information exchange. In short, making connectivity succeed depends on a multi-stakeholder collaboration no matter the discipline or transactional sector.

Technical measures should support safe end-user access.

Government policymakers should think about flexible policy measures that enable the private sector to innovate in the creation and delivery of technologies and services that promote secure connectivity. The case of Estonia's national ID-card system demonstrates that technical remedies can be employed to promote and support end-user security. It provides a robust layer of protection for access to financial and government services, ranging from to tax filing to voting to the use of health services. The system applies simple but resilient principles of public key cryptography. Moreover -- and remarkably, in comparison to similar national ID-card schemes -- the Estonian system records all requests for user data, which facilitates the detection and forensic investigation of unauthorized or inappropriate access.

29 National eHealth Collaborative (NeHC) is a public-private partnership that enables secure and interoperable nationwide health information exchange to advance health and improve healthcare. See more at: http://www.nationalehealth.org/about-national-ehealth-collaborative#sthash.uTz6Ym9f.dpuf

2

TRUST

Transparent terms of the government-citizen online relationship are an essential part of a trusted internet ecosystem.

In the end, online trust is about more than user-verification and consumer protection policy. Agreement on transparent standards of appropriate state behavior online -- particularly with respect to the appropriate balance between national security and user privacy -- is of utmost importance in creating a trusted ecosystem. However, this cannot involve just the governments themselves: given the role of the private sector in developing, refining and operationalizing existing confidence-building measures (eg vulnerability disclosure management, secure development of code and adequate reporting of government requests for user data), it is only reasonable that industry and citizen representatives be included in the effort. A public-private partnership on this important issue offers the most comprehensive and sustainable approach to developing confidence-building measures.

Developing transparent confidence-building measures between governments is fundamental to long-term trust.

Cybersecurity has emerged as a serious international diplomatic issue as political leaders grapple with how to establish norms or delineate the accountability of national governments for cross-border cyberattacks. These issues will only gain in prominence in bilateral and multilateral relationships. Government policymakers need to work internationally to develop agreement on cybersecurity norms and focus on practical measures to enhance coordination and cooperation. It is likely that progress will be incremental with regular flare-ups as new hacking attempts occur -- however, increased effort on international standards can help build trust between nations and avoid dangerous miscalculations or misjudgements that lead to conflict.

1

OPTIMUM

Sustaining optimum security requires constant adaptability and preparedness.

No government can afford cybersecurity complacency or isolation. Government policymakers need to work with the private sector to understand changes in the threat landscape and support the development of new approaches to cybersecurity risk management and preparedness. The threat landscape in cyberspace is constantly changing. For this reason, the essential precondition of effective cyber risk management for the preservation of the optimum state -- once it is achieved -- is the ability to adapt to novel and unexpected security challenges. In short, adaptability is the cornerstone of preparedness.

Adapting a learning stance on cybersecurity will help achieve and maintain a state where the internet is being used to its full potential.

In a related point to the above, governments must constantly seek out new learning, best practices and lessons from failures to build an ever-more robust system. It is often said that the only thing we know about the future is that it will not be like the past: this means the governments best placed to secure the internet for the wellbeing of the country are those that remain future-oriented. Developing access, improving resilience, building connectivity and strengthening user trust are ongoing pursuits -- meeting these needs depends on evolving national contexts, emerging technological developments and innovations on the horizon that we cannot yet know. Attacks will persist and breaches will occur, but the governments that use these incidents as a feedback loop to constantly enforce and refresh their cybersecurity postures will be the most successful in continuing to meet the needs of the hierarchy.

Oxford Analytica

HEAD OFFICE
5 Alfred Street, Oxford OX1 4EH
T +44 1865 261 600

USA
1069 Thomas Jefferson Street, NW
Washington DC 20007
T +1 202 342 2860

405 Lexington Avenue, Suite 54B
New York, NY 10174
T +1 646 430 9014

FRANCE
5, Rue de Surène, 75008 Paris
T +33 1 42 89 08 36

www.oxan.com